# Cisco NCS 4200 Series Software Configuration Guide, Cisco IOS XE 16

**First Published:** 2017-05-05

**Last Modified:** 2020-04-16

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

CHAPTER 1

# Feature History

The following table lists the new and modified features supported in the Cisco NCS 4200 Series Software Configuration Guide in Cisco IOS XE 16 releases, on Cisco NCS 4201 and Cisco NCS 4202 routers.

| Feature Name | Cisco IOS XE Release |
|---|---|
| Video Template - IPv4 QoS classifications | 16.11.1a |
| PTP Asymmetry Readjustment | |
| Zero Touch Provisioning | |
| SNMP Dying Gasp Support | 16.9.4 |
| RS232 Sync | 16.9.1a |
| 1 PPS Pulse Width Configuration | 16.6.1 |
| Alarm support for 900W | |
| Unframed E1 for BCP over MLPPP | 16.5.1 |
| G.8275.2 Telecom Profile | |

The following table lists the new and modified features supported in the Cisco NCS 4200 Series Software Configuration Guide in Cisco IOS XE 16 releases, on Cisco NCS 4206 and Cisco NCS 4216 routers.

| Feature Name | Cisco IOS XE Release |
|---|---|
| Video Template - IPv4 QoS classifications | 16.11.1a |
| PTP Asymmetry Readjustment | |
| Zero Touch Provisioning | |
| SDM template enhancement for uRPF scale | 16.9.4 |

| Feature Name | Cisco IOS XE Release |
|---|---|
| Dying GASP via SNMP trap | 16.9.1a |
| RS232 Sync | |
| Over Subscription Mode and Partial Port Mode Support on 8-port 10 Gigabit Ethernet Interface Module on NCS 4216 Chassis | |
| Card Protection for 48-port T1/E1 CEM Interface Module and 48-port T3/E3 CEM Interface Module | 16.6.1 |
| DS1 and DS3 Card Protection | |
| 1 PPS Pulse Width Configuration | |
| G.8275.2 Telecom Profile | 16.5.1 |
| OTN Wrapper | |

CHAPTER 2

# Using Cisco IOS XE Software



## Understanding Command Modes

The command modes available in the traditional Cisco IOS CLI are exactly the same as the command modes available in Cisco IOS XE.

You use the CLI to access Cisco IOS XE software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode, you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS XE software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

Table 1: Accessing and Exiting Command Modes , on page 4 describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.

*Table 1: Accessing and Exiting Command Modes*

| Command Mode | Access Method | Prompt | Exit Method |
|---|---|---|---|
| User EXEC | Log in. | `Router>` | Use the **logout** command. |
| Privileged EXEC | From user EXEC mode, use the **enable** EXEC command. | `Router#` | To return to user EXEC mode, use the **disable** command. |
| Global configuration | From privileged EXEC mode, use the **configure terminal** privileged EXEC command. | `Router(config)#` | To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command. |
| Interface configuration | From global configuration mode, specify an interface using an **interface** command. | `Router(config-if)#` | To return to global configuration mode, use the **exit** command.<br>To return to privileged EXEC mode, use the **end** command. |
| Diagnostic | The router boots up or accesses diagnostic mode in the following scenarios:<br>• In some cases, diagnostic mode will be reached when the IOS process or processes fail. In most scenarios, however, the router will reload.<br>• A user-configured access policy was configured using the **transport-map** command that directed the user into diagnostic mode. See the Using Cisco IOS XE Software, on page 3 chapter of this book for information on configuring access policies.<br>• The router was accessed using a Route Switch Processor auxiliary port.<br>• A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command ) was entered and the router was configured to go into diagnostic mode when the break signal was received. | `Router(diag)#` | If the IOS process failing is the reason for entering diagnostic mode, the IOS problem must be resolved and the router rebooted to get out of diagnostic mode.<br>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.<br>If the router is accessed through the Route Switch Processor auxiliary port, access the router through another port. Accessing the router through the auxiliary port is not useful for customer purposes anyway. |

| Command Mode | Access Method | Prompt | Exit Method |
|---|---|---|---|
| ROM monitor | From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting. | > | To exit ROM monitor mode, use the **continue** command. |

### Universal IOS Image

Starting with XE318SP, there are two flavors of universal images supported on Cisco ASR900 series routers:

- Universal images with the "universalk9" designation in the image name: This universal image offers the strong payload cryptography Cisco IOS feature, the IPSec VPN feature.
- Universal images with the universalk9_npe" designation in the image name: The strong enforcement of encryption capabilities provided by Cisco Software Activation satisfies requirements for the export of encryption capabilities. However, some countries have import requirements that require that the platform does not support any strong crypto functionality such as payload cryptography. To satisfy the import requirements of those countries, the `npe' universal image does not support any strong payload encryption.

Starting with Cisco IOS XE Release 3.18SP, IPsec tunnel is supported only on the Cisco ASR903 and ASR907 routers with payload encryption (PE) images. IPSec requires an IPsec license to function.

**Note**

- IPsec license must be acquired and installed in the router for IPsec functionality to work. When you enable or disable the IPsec license, reboot is mandatory for the system to function properly. IPsec is not supported on Cisco IOS XE Everest 16.5.1.
- NPE images shipped for Cisco ASR 900 routers do not support data plane encryptions. However, control plane encryption is supported with NPE images, with processing done in software, without the crypto engine.

# Understanding Diagnostic Mode

Diagnostic mode is supported.

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the RSP will simply reset when the IOS process or processes fail.
- A user-configured access policy was configured using the **transport-map** command that directs the user into diagnostic mode.
- A send break signal (**Ctrl-C** or **Ctrl-Shift-6**) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

In diagnostic mode, a subset of the commands that are also available in User EXEC mode are made available to users. Among other things, these commands can be used to:

- Inspect various states on the router, including the IOS state.
- Replace or roll back the configuration.

- Provide methods of restarting the IOS or other processes.
- Reboot hardware, such as the entire router, an RSP, an IM, or possibly other hardware components.
- Transfer files into or off of the router using remote access methods such as FTP, TFTP, SCP, and so on.

The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMmon, to diagnose and troubleshoot IOS problems.

The diagnostic mode commands are stored in the non-IOS packages on the chassis, which is why the commands are available even if the IOS process is not working properly. Importantly, all the commands available in diagnostic mode are also available in privileged EXEC mode on the router even during normal router operation. The commands are entered like any other commands in the privileged EXEC command prompts when used in privileged EXEC mode.

# Accessing the CLI Using a Console

The following sections describe how to access the command-line interface (CLI) using a directly-connected console or by using Telnet or a modem to obtain a remote console:

## Accessing the CLI Using a Directly-Connected Console

This section describes how to connect to the console port on the router and use the console interface to access the CLI. The console port is located on the front panel of each Route Switch Processor (RSP).

### Connecting to the Console Port

Before you can use the console interface on the router using a terminal or PC, you must perform the following steps:

**Procedure**

---

**Step 1** Configure your terminal emulation software with the following settings:

- 9600 bits per second (bps)
- 8 data bits
- No parity
- 1 stop bit
- No flow control

**Step 2** Connect to the port using the RJ-45-to-RJ-45 cable and RJ-45-to-DB-25 DTE adapter or using the RJ-45-to-DB-9 DTE adapter (labeled “Terminal”).

---

### Using the Console Interface

Every RSP has a console interface. Notably, a standby RSP can be accessed using the console port in addition to the active RSP in a dual RSP configuration.

To access the CLI using the console interface, complete the following steps:

**Procedure**

**Step 1** After you attach the terminal hardware to the console port on the router and you configure your terminal emulation software with the proper settings, the following prompt appears:

**Example:**

```
Press RETURN to get started.
```

**Step 2** Press **Return** to enter user EXEC mode. The following prompt appears:

**Example:**

```
Router>
```

**Step 3** From user EXEC mode, enter the **enable** command as shown in the following example:

**Example:**

```
Router> enable
```

**Step 4** At the password prompt, enter your system password. If an enable password has not been set on your system, this step may be skipped.The following example shows entry of the password called "enablepass":

**Example:**

```
Password: enablepass
```

**Step 5** When your enable password is accepted, the privileged EXEC mode prompt appears:

**Example:**

```
Router#
```

**Step 6** You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

**Step 7** To exit the console session, enter the **exit** command as shown in the following example:

**Example:**

```
Router# exit
```

# Accessing the CLI from a Remote Console Using Telnet

This section describes how to connect to the console interface on a router using Telnet to access the CLI.

## Preparing to Connect to the Router Console Using Telnet

Before you can access the router remotely using Telnet from a TCP/IP network, you need to configure the router to support virtual terminal lines (vtys) using the **line vty** global configuration command. You also should configure the vtys to require login and specify a password.

**Note** To prevent disabling login on the line, be careful that you specify a password with the **password** command when you configure the **login** line configuration command. If you are using authentication, authorization, and accounting (AAA), you should configure the **login authentication** line configuration command. To prevent disabling login on the line for AAA authentication when you configure a list with the **login authentication** command, you must also configure that list using the **aaa authentication login** global configuration command. For more information about AAA services, refer to the *Cisco IOS XE Security Configuration Guide,* Release 2 and *Cisco IOS Security Command Reference* publications.

In addition, before you can make a Telnet connection to the router, you must have a valid host name for the router or have an IP address configured on the router. For more information about requirements for connecting to the router using Telnet, information about customizing your Telnet services, and using Telnet key sequences, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide,* Release 12.2SR.

## Using Telnet to Access a Console Interface

To access a console interface using Telnet, complete the following steps:

### Procedure

**Step 1** From your terminal or PC, enter one of the following commands:

- **connect** *host* [*port*] [*keyword*]
- **telnet** *host* [*port*] [*keyword*]

In this syntax, *host* is the router hostname or an IP address, *port* is a decimal port number (23 is the default), and *keyword* is a supported keyword. For more information, refer to the *Cisco IOS Configuration Fundamentals Command Reference* .

**Note** If you are using an access server, then you will need to specify a valid port number such as **telnet 172.20.52.40 2004**, in addition to the hostname or IP address.

The following example shows the **telnet** command to connect to the router named “router”:

**Example:**

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

**Step 2** At the password prompt, enter your login password. The following example shows entry of the password called “mypass”:

**Example:**

```
User Access Verification
Password: mypass
```

**Note** If no password has been configured, press **Return**.

**Step 3** From user EXEC mode, enter the **enable** command as shown in the following example:

**Example:**

```
Router> enable
```

**Step 4** At the password prompt, enter your system password. The following example shows entry of the password called "enablepass":

**Example:**

```
Password: enablepass
```

**Step 5** When the enable password is accepted, the privileged EXEC mode prompt appears:

**Example:**

```
Router#
```

**Step 6** You now have access to the CLI in privileged EXEC mode and you can enter the necessary commands to complete your desired tasks.

**Step 7** To exit the Telnet session, use the **exit** or **logout** command as shown in the following example:

**Example:**

```
Router# logout
```

## Accessing the CLI from a Remote Console Using a Modem

To access the router remotely using a modem through an asynchronous connection, connect the modem to the console port.

The console port on a chassis is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is located on the front panel of the RSP.

To connect a modem to the console port, place the console port mode switch in the in position. Connect to the port using the RJ-45-to-RJ-45 cable and the RJ-45-to-DB-25 DCE adapter (labeled "Modem").

To connect to the router using the USB console port, connect to the port using a USB Type A-to-Type A cable.

# Using the Auxiliary Port

The auxiliary port on the Route Switch Processor does not serve any useful purpose for customers.

This port should only be accessed under the advisement of a customer support representative.

# Using Keyboard Shortcuts

Commands are not case sensitive. You can abbreviate commands and parameters if the abbreviations contain enough letters to be different from any other currently available commands or parameters.

Table 2: Keyboard Shortcuts , on page 10 lists the keyboard shortcuts for entering and editing commands.

*Table 2: Keyboard Shortcuts*

| Keystrokes | Purpose |
|---|---|
| **Ctrl-B** or the **Left Arrow** key[1] | Move the cursor back one character |
| **Ctrl-F** orthe **Right Arrow** key1 | Move the cursor forward one character |
| **Ctrl-A** | Move the cursor to the beginning of the command line |
| **Ctrl-E** | Move the cursor to the end of the command line |
| **Esc B** | Move the cursor back one word |
| **Esc F** | Move the cursor forward one word |

1 The arrow keys function only on ANSI-compatible terminals such as VT100s.

# Using the History Buffer to Recall Commands

The history buffer stores the last 20 commands you entered. History substitution allows you to access these commands without retyping them, by using special abbreviated commands.

Table 3: History Substitution Commands, on page 10 lists the history substitution commands.

*Table 3: History Substitution Commands*

| Command | Purpose |
|---|---|
| **Ctrl-P** or the **Up Arrow** key[2] | Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands. |
| **Ctrl-N** or the **Down Arrow** key1 | Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the **Up Arrow** key. |
| `Router#` **`show history`** | While in EXEC mode, list the last several commands you have just entered. |

2 The arrow keys function only on ANSI-compatible terminals such as VT100s.

# Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

*Table 4: Help Commands and Purpose*

| Command | Purpose |
|---|---|
| **help** | Provides a brief description of the help system in any command mode. |
| *abbreviated-command-entry* **?** | Provides a list of commands that begin with a particular character string. (No space between command and question mark.) |
| *abbreviated-command-entry* <**Tab** > | Completes a partial command name. |
| **?** | Lists all commands available for a particular command mode. |
| *command* **?** | Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.) |

# Finding Command Options Example

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS XE software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **rep** command, you would type **rep ?**.

The <cr> symbol in command help output stands for "carriage return." On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 5: Finding Command Options , on page 11 shows examples of how you can use the question mark (**?**) to assist you in entering commands.

*Table 5: Finding Command Options*

| Command | Comment |
|---|---|
| Router> **enable**<br>Password: *<password>*<br>Router# | Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a "# " from the "> "; for example, Router> to Router# . |

<table>
<tr><th>Command</th><th>Comment</th></tr>
<tr><td><pre>Router#
configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#</pre></td><td>Enter the configure terminal privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)# .</td></tr>
<tr><td><pre>Router(config)# interface gigabitEthernet ?
  <0-0>  GigabitEthernet interface number
  <0-1>  GigabitEthernet interface number
Router(config)#interface gigabitEthernet 0?
.  /  <0-0>
Router(config)#interface gigabitEthernet 0/?
  <0-5>  Port Adapter number
Router(config)#interface gigabitEthernet 0/0?
/
Router(config)#interface gigabitEthernet 0/0/?
  <0-15>  GigabitEthernet interface number
Router(config)#interface gigabitEthernet 0/0/0?
.  <0-23>
Router(config)#interface gigabitEthernet 0/0/0</pre></td><td>Enter interface configuration mode by specifying the serial interface that you want to configure using the interface serial global configuration command.<br><br>Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.<br><br>When the <cr> symbol is displayed, you can press Enter to complete the command.<br><br>You are in interface configuration mode when the prompt changes to Router(config-if)# .</td></tr>
<tr><td><pre>Router(config-if)# ?
Interface configuration commands:
  .
  .
  .
  ip                 Interface Internet Protocol config
 commands
  keepalive           Enable keepalive
  lan-name            LAN Name command
  llc2                LLC2 Interface Subcommands
  load-interval       Specify interval for load
calculation for an
                      interface
  locaddr-priority    Assign a priority group
  logging             Configure logging for interface
  loopback           Configure internal loopback on an
 interface
  mac-address        Manually set interface MAC address

  mls                 mls router sub/interface commands

  mpoa                MPOA interface configuration
commands
  mtu                 Set the interface Maximum
Transmission Unit (MTU)
  netbios            Use a defined NETBIOS access list
 or enable
                      name-caching
  no                  Negate a command or set its
defaults
  nrzi-encoding       Enable use of NRZI encoding
  ntp                 Configure NTP
  .
  .
  .
Router(config-if)#</pre></td><td>Enter ? to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.</td></tr>
</table>

<table>
<tr><th>Command</th><th>Comment</th></tr>
<tr><td><pre>
Router(config-if)# ip ?
Interface IP configuration subcommands:
  access-group       Specify access control for packets

  accounting         Enable IP accounting on this
interface
  address            Set the IP address of an interface

  authentication     authentication subcommands
  bandwidth-percent  Set EIGRP bandwidth limit
  broadcast-address  Set the broadcast address of an
interface
  cgmp               Enable/disable CGMP
  directed-broadcast Enable forwarding of directed
broadcasts
  dvmrp              DVMRP interface commands
  hello-interval     Configures IP-EIGRP hello interval

  helper-address     Specify a destination address for
 UDP broadcasts
  hold-time          Configures IP-EIGRP hold time
  .
  .
  .
Router(config-if)# ip
</pre></td><td>Enter the command that you want to configure for the interface. This example uses the ip command.<br><br>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</td></tr>
<tr><td><pre>
Router(config-if)# ip address ?
  A.B.C.D            IP address
  negotiated         IP Address negotiated over PPP
Router(config-if)# ip address
</pre></td><td>Enter the command that you want to configure for the interface. This example uses the ip address command.<br><br>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP address or the negotiated keyword.<br><br>A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</td></tr>
<tr><td><pre>
Router(config-if)# ip address 172.16.0.1 ?
  A.B.C.D            IP subnet mask
Router(config-if)# ip address 172.16.0.1
</pre></td><td>Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.<br><br>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.<br><br>A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</td></tr>
<tr><td><pre>
Router(config-if)# ip address 172.16.0.1 255.255.255.0
?
  secondary          Make this IP address a secondary
address
  <cr>
Router(config-if)# ip address 172.16.0.1 255.255.255.0
</pre></td><td>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.<br><br>Enter ? to display what you must enter next on the command line. In this example, you can enter the secondary keyword, or you can press Enter.<br><br>A <cr> is displayed; you can press Enter to complete the command, or you can enter another keyword.</td></tr>
</table>

| Command | Comment |
|---|---|
| Router(config-if)# **ip address 172.16.0.1 255.255.255.0**<br>Router(config-if)# | In this example, **Enter** is pressed to complete the command. |

# Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to re-enable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Many CLI commands also have a **default** form. By issuing the command **default** *command-name* , you can configure the command to its default setting. The Cisco IOS software command reference publications describe the function of the **default** form of the command when the **default** form performs a different function than the plain and **no** forms of the command. To see what default commands are available on your system, enter **default ?** in the appropriate command mode.

# Saving Configuration Changes

Use the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

This task saves the configuration to NVRAM.

# Managing Configuration Files

On the chassis, the startup configuration file is stored in the nvram: file system and the running-configuration files are stored in the system: file system. This configuration file storage setup is not unique to the chassis and is used on several Cisco router platforms.

As a matter of routine maintenance on any Cisco router, users should backup the startup configuration file by copying the startup configuration file from NVRAM onto one of the router's other file systems and, additionally, onto a network server. Backing up the startup configuration file provides an easy method of recovering the startup configuration file in the event the startup configuration file in NVRAM becomes unusable for any reason.

The **copy** command can be used to backup startup configuration files. Below are some examples showing the startup configuration file in NVRAM being backed up:

#### Example 1: Copying Startup Configuration File to Bootflash

```
Router# dir bootflash:
Directory of bootflash:/
   11  drwx       16384   Feb 2 2000 13:33:40 +05:30  lost+found
15105  drwx        4096   Feb 2 2000 13:35:07 +05:30  .ssh
45313  drwx        4096  Nov 17 2011 17:36:12 +05:30  core
75521  drwx        4096   Feb 2 2000 13:35:11 +05:30  .prst_sync
90625  drwx        4096   Feb 2 2000 13:35:22 +05:30  .rollback_timer
105729  drwx        8192  Nov 21 2011 22:57:55 +05:30  tracelogs
30209  drwx        4096   Feb 2 2000 13:36:17 +05:30  .installer
1339412480 bytes total (1199448064 bytes free)
Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?
3517 bytes copied in 0.647 secs (5436 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/
   11  drwx       16384   Feb 2 2000 13:33:40 +05:30  lost+found
15105  drwx        4096   Feb 2 2000 13:35:07 +05:30  .ssh
45313  drwx        4096  Nov 17 2011 17:36:12 +05:30  core
75521  drwx        4096   Feb 2 2000 13:35:11 +05:30  .prst_sync
90625  drwx        4096   Feb 2 2000 13:35:22 +05:30  .rollback_timer
   12  -rw-           0   Feb 2 2000 13:36:03 +05:30  tracelogs.878
105729  drwx        8192  Nov 21 2011 23:02:13 +05:30  tracelogs
30209  drwx        4096   Feb 2 2000 13:36:17 +05:30  .installer
   13  -rw-        1888  Nov 21 2011 23:03:17 +05:30  startup-config
1339412480 bytes total (1199439872 bytes free)
```

#### Example 2: Copying Startup Configuration File to USB Flash Disk

```
Router# dir usb0:
Directory of usb0:/
43261  -rwx   208904396  May 27 2008 14:10:20 -07:00
ncs4200rsp3-adventerprisek9.02.01.00.122-33.XNA.bin
255497216 bytes total (40190464 bytes free)
Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?
3172 bytes copied in 0.214 secs (14822 bytes/sec)
Router# dir usb0:
Directory of usb0:/
43261  -rwx   208904396  May 27 2008 14:10:20 -07:00
ncs4200rsp3-adventerprisek9.02.01.00.122-33.XNA.bin43262 -rwx
 3172 Jul 2 2008 15:40:45 -07:00  startup-config255497216 bytes total (40186880 bytes free)
```

#### Example 3: Copying Startup Configuration File to a TFTP Server

```
Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_confg]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)
```

For more detailed information on managing configuration files, see the *Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S* .

# Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character ( | ); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case sensitive):

**show** *command* | {**append** | **begin** | **exclude** | **include** | **redirect** | **section** | **tee** | **count**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is up, line protocol is up
Serial4/0/0 is up, line protocol is up
Serial4/1/0 is up, line protocol is up
Serial4/2/0 is administratively down, line protocol is down
Serial4/3/0 is administratively down, line protocol is down
```

# Powering Off the Router

Before you turn off a power supply, make certain the chassis is grounded and you perform a soft shutdown on the power supply. Not performing a soft shutdown will often not harm the router, but may cause problems in certain scenarios.

To perform a soft shutdown before powering off the router, enter the **reload** command to halt the system and then wait for ROM Monitor to execute before proceeding to the next step.

The following screenshot shows an example of this process:

```
Router# reload
Proceed with reload? [confirm]
*Jun 18 19:38:21.870: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
command.
```

Place the power supply switch in the Off position after seeing this message.

# Finding Support Information for Platforms and Cisco Software Images

Cisco software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS XE software image, you can use Cisco Feature Navigator or the software release notes.

# Using Cisco Feature Navigator

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

# Using Software Advisor

To see if a feature is supported by a Cisco IOS XE release, to locate the software document for that feature, or to check the minimum software requirements of Cisco IOS XE software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com at http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl.

You must be a registered user on Cisco.com to access this tool.

# Using Software Release Notes

Cisco IOS XE software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- New feature information
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. Refer to Cisco Feature Navigator for cumulative feature information.

CHAPTER 3

# Console Port Telnet and SSH Handling

This chapter covers the following topics:



## Important Notes and Restrictions

- The Telnet and SSH settings made in the transport map override any other Telnet or SSH settings when the transport map is applied to the Management Ethernet interface.
- Only local usernames and passwords can be used to authenticate users entering a Management Ethernet interface. AAA authentication is not available for users accessing the router through a Management Ethernet interface using persistent Telnet or persistent SSH.
- Applying a transport map to a Management Ethernet interface with active Telnet or SSH sessions can disconnect the active sessions. Removing a transport map from an interface, however, does not disconnect any active Telnet or SSH sessions.
- Configuring the diagnostic and wait banners i s optional but recommended. The banners are especially useful as indicators to users of the status of their Telnet or SSH attempts.

## Console Port Overview

The console port on the chassis is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is used to access the chassis and is located on the front panel of the Route Switch Processor (RSP).

For information on accessing the chassis using the console port, see the "Accessing the CLI Using a Console" section on page 1-4 .

# Connecting Console Cables

For information about connecting console cables to the chassis, see the NCS 4200 Hardware Installation Guides.

# Installing USB Device Drivers

For instructions on how to install device drivers in order to use the USB console port, see the NCS 4200 Hardware Installation Guides.

# Console Port Handling Overview

Users using the console port to access the chassis are automatically directed to the IOS command-line interface, by default.

If a user is trying to access the router through the console port and sends a break signal (a break signal can be sent by entering **Ctrl-C** or **Ctrl-Shift-6**, or by entering the **send break** command at the Telnet prompt ) before connecting to the IOS command-line interface, the user is directed into diagnostic mode by default if the non-RPIOS sub-packages can be accessed.

These settings can be changed by configuring a transport map for the console port and applying that transport map to the console interface.

# Telnet and SSH Overview

Telnet and Secure Shell (SSH) can be configured and handled like Telnet and SSH on other Cisco platforms. For information on traditional Telnet, see the **line** command in the *Cisco IOS Terminal Services Command Reference guide* located at http://www.cisco.com/en/US/docs/ios/12_2/termserv/command/reference/trflosho.html#wp1029818.

For information on configuring traditional SSH, see the Secure Shell Configuration Guide, Cisco IOS XE Release 3S

The chassis also supports persistent Telnet and persistent SSH. Persistent Telnet and persistent SSH allow network administrators to more clearly define the treatment of incoming traffic when users access the router through the Management Ethernet port using Telnet or SSH. Notably, persistent Telnet and persistent SSH provide more robust network access by allowing the router to be configured to be accessible through the Ethernet Management port using Telnet or SSH even when the IOS process has failed.

# Persistent Telnet and Persistent SSH Overview

In traditional Cisco routers, accessing the router using Telnet or SSH is not possible in the event of an IOS failure. When Cisco IOS fails on a traditional Cisco router, the only method of accessing the router is through the console port. Similarly, if all active IOS processes have failed on a chassis that is not using persistent Telnet or persistent SSH, the only method of accessing the router is through the console port.

With persistent Telnet and persistent SSH, however, users can configure a transport map that defines the treatment of incoming Telnet or SSH traffic on the Management Ethernet interface. Among the many configuration options, a transport map can be configured to direct all traffic to the IOS command-line interface, diagnostic mode, or to wait for an IOS vty line to become available and then direct users into diagnostic mode when the user sends a break signal while waiting for the IOS vty line to become available. If a user uses Telnet or SSH to access diagnostic mode, that Telnet or SSH connection will be usable even in scenarios when no IOS process is active. Therefore, persistent Telnet and persistent SSH introduce the ability to access the router via diagnostic mode when the IOS process is not active. For information on diagnostic mode, see the "Understanding Diagnostic Mode" section on page 1-3 .

For more information on the various other options that are configurable using persistent Telnet or persistent SSH transport map see the Configuring Persistent Telnet, on page 23 and the Configuring Persistent SSH, on page 25 .

# Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **transport-map type console** ***transport-map-name***<br>**Example:**<br>`Router(config)# transport-map type console consolehandler` | Creates and names a transport map for handling console connections, and enter transport map configuration mode. |
| **Step 4** | **connection wait** [**allow interruptible** \| **none**]<br>**Example:**<br>`Router(config-tmap)# connection wait none`<br>**Example:** | Specifies how a console connection will be handled using this transport map:<br>• **allow interruptible**—The console connection waits for an IOS vty line to become available, and also allows user to enter diagnostic mode by interrupting a console connection waiting for the IOS vty |

| | Command or Action | Purpose |
|---|---|---|
| | | line to become available. This is the default setting.<br>**Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.<br>• **none**—The console connection immediately enters diagnostic mode. |
| **Step 5** | **banner** [**diagnostic** \| **wait**] *banner-message*<br>**Example:**<br>`Router(config-tmap)# banner diagnostic X`<br>**Example:**<br>`Enter TEXT message.  End with the character 'X'.`<br>**Example:**<br>`--Welcome to Diagnostic Mode--`<br>**Example:**<br>`X`<br>**Example:**<br>`Router(config-tmap)#`<br>**Example:** | (Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS vty line as a result of the console transport map configuration.<br>• **diagnostic**—Creates a banner message seen by users directed into diagnostic mode as a result of the console transport map configuration.<br>• **wait**—Creates a banner message seen by users waiting for the IOS vty to become available.<br>• *banner-message*—The banner message, which begins and ends with the same delimiting character. |
| **Step 6** | **exit**<br>**Example:**<br>`Router(config-tmap)# exit` | Exits transport map configuration mode to re-enter global configuration mode. |
| **Step 7** | **transport type console** *console-line-number* **input** *transport-map-name*<br>**Example:**<br>`Router(config)# transport type console 0 input consolehandler` | Applies the settings defined in the transport map to the console interface.<br>The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** comm and. |

# Examples

In the following example, a transport map to set console port access policies is created and attached to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
Welcome to diagnostic mode
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

# Configuring Persistent Telnet

### Before you begin

For a persistent Telnet connection to access an IOS vty line on the chassis, local login authentication must be configured for the vty line (the **login** command in line configuration mode). If local login authentication is not configured, users will not be able to access IOS using a Telnet connection into the Management Ethernet interface with an applied transport map. Diagnostic mode will still be accessible in this scenario.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **transport-map type persistent telnet** *transport-map-name*<br>**Example:**<br>`Router(config)# transport-map type persistent telnet telnethandler` | Creates and names a transport map for handling persistent Telnet connections, and enters transport map configuration mode. |
| **Step 4** | **connection wait** [**allow** {**interruptible**}\| **none** {**disconnect**}]<br>**Example:**<br>`Router(config-tmap)# connection wait none`<br>**Example:** | Specifies how a persistent Telnet connection will be handled using this transport map:<br>• **allow**—The Telnet connection waits for an IOS vty line to become available, and exits the router if interrupted.<br>• **allow interruptible**—The Telnet connection waits for the IOS vty line to |

| | Command or Action | Purpose |
|---|---|---|
| | | become available, and also allows user to enter diagnostic mode by interrupting a Telnet connection waiting for the IOS vty line to become available. This is the default setting.<br>**Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.<br>• **none**—The Telnet connection immediately enters diagnostic mode.<br>• **none disconnect**—The Telnet connection does not wait for the IOS vty line and does not enter diagnostic mode, so all Telnet connections are rejected if no vty line is immediately available in IOS. |
| **Step 5** | **banner** [**diagnostic** \| **wait**] *banner-message*<br>**Example:**<br>`Router(config-tmap)# banner diagnostic X`<br>**Example:**<br>`Enter TEXT message.  End with the character 'X'.`<br>**Example:**<br>`--Welcome to Diagnostic Mode--`<br>**Example:**<br>`X`<br>**Example:**<br>`Router(config-tmap)#`<br>**Example:** | (Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the IOS vty line as a result of the persistent Telnet configuration.<br>• **diagnostic**—creates a banner message seen by users directed into diagnostic mode as a result of the persistent Telnet configuration.<br>• **wait**—creates a banner message seen by users waiting for the vty line to become available.<br>• *banner-message*—the banner message, which begins and ends with the same delimiting character. |
| **Step 6** | **transport interface type** *num*<br>**Example:**<br>`Router(config-tmap)# transport interface gigabitethernet 0` | Applies the transport map settings to the Management Ethernet interface (interface gigabitethernet 0).<br>Persistent Telnet can only be applied to the Management Ethernet interface on the chassis. This step must be taken before applying the transport map to the Management Ethernet interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **exit**<br>**Example:**<br>`Router(config-tmap)# exit` | Exits transport map configuration mode to re-enter global configuration mode. |
| **Step 8** | **transport type persistent telnet input** *transport-map-name*<br>**Example:**<br>`Router(config)# transport type persistent telnet input telnethandler` | Applies the settings defined in the transport map to the Management Ethernet interface.<br>The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type persistent telnet** comm and. |

## Examples

In the following example, a transport map that will make all Telnet connections wait for an IOS vty line to become available before connecting to the router, while also allowing the user to interrupt the process and enter diagnostic mode, is configured and applied to the Management Ethernet interface (interface gigabitethernet 0).

A diagnostic and a wait banner are also configured.

The transport map is then applied to the interface when the **transport type persistent telnet input** command is entered to enable persistent Telnet.

```
Router(config)# transport-map type persistent telnet telnethandler
Router(config-tmap)#
connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for IOS Process--
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

# Configuring Persistent SSH

This task describes how to configure persistent SSH.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:** | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router> enable` | |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **transport-map type persistent ssh** *transport-map-name*<br>**Example:**<br>`Router(config)# transport-map type persistent ssh sshhandler` | Creates and names a transport map for handling persistent SSH connections, and enters transport map configuration mode. |
| **Step 4** | **connection wait** [**allow** {**interruptible**}\| **none** {**disconnect**}]<br>**Example:**<br>`Router(config-tmap)# connection wait allow interruptible`<br>**Example:** | Specifies how a persistent SSH connection will be handled using this transport map:<br>• **allow**—The SSH connection waits for the vty line to become available, and exits the router if interrupted.<br>• **allow interruptible**—The SSH connection waits for the vty line to become available, and also allows users to enter diagnostic mode by interrupting a SSH connection waiting for the vty line to become available. This is the default setting.<br>**Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.<br>• **none**—The SSH connection immediately enters diagnostic mode.<br>• **none disconnect**—The SSH connection does not wait for the vty line from IOS and does not enter diagnostic mode, so all SSH connections are rejected if no vty line is immediately available. |
| **Step 5** | **rsa keypair-name** *rsa-keypair-name*<br>**Example:**<br>`Router(config-tmap)# rsa keypair-name sshkeys` | Names the RSA keypair to be used for persistent SSH connections.<br>For persistent SSH connections, the RSA keypair name must be defined using this command in transport map configuration mode. The RSA keypair definitions defined elsewhere on the router, such as through the use of the **ip ssh rsa keypair-name** command, do not apply to persistent SSH connections. |

| | Command or Action | Purpose |
|---|---|---|
| | | No *rsa-keypair-name* is defined by default. |
| **Step 6** | **authentication-retries***number-of-retries*<br>**Example:**<br>`Router(config-tmap)# authentication-retries 4` | (Optional) Specifies the number of authentication retries before dropping the connection.<br>The default *number-of-retries* is 3. |
| **Step 7** | **banner** [**diagnostic** \| **wait**] *banner-message*<br>**Example:**<br>`Router(config-tmap)# banner diagnostic X`<br>**Example:**<br>`Enter TEXT message.  End with the character 'X'.`<br>**Example:**<br>`--Welcome to Diagnostic Mode--`<br>**Example:**<br>`X`<br>**Example:**<br>`Router(config-tmap)#` | (Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the vty line as a result of the persistent SSH configuration.<br>• **diagnostic**—Creates a banner message seen by users directed into diagnostic mode as a result of the persistent SSH configuration.<br>• **wait**—Creates a banner message seen by users waiting for the vty line to become active.<br>• *banner-message*—The banner message, which begins and ends with the same delimiting character. |
| **Step 8** | **time-out***timeout-interval*<br>**Example:**<br>`Router(config-tmap)# time-out 30` | (Optional) Specifies the SSH time-out interval in seconds.<br>The default *timeout-interval* is 120 seconds. |
| **Step 9** | **transport interface type** *num*<br>**Example:**<br>`Router(config-tmap)# transport interface gigabitethernet 0` | Applies the transport map settings to the Management Ethernet interface (interface gigabitethernet 0).<br>Persistent SSH can only be applied to the Management Ethernet interface on the chassis. |
| **Step 10** | **exit**<br>**Example:**<br>`Router(config-tmap)# exit` | Exits transport map configuration mode to re-enter global configuration mode. |
| **Step 11** | **transport type persistent ssh input** *transport-map-name*<br>**Example:** | Applies the settings defined in the transport map to the Management Ethernet interface.<br>The *transport-map-name* for this command must match the *transport-map-name* defined |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config)# transport type persistent ssh input sshhandler` | in the **transport-map type persistent ssh** command . |

# Examples

In the following example, a transport map that will make all SSH connections wait for the vty line to become active before connecting to the router is configured and applied to the Management Ethernet interface (interface gigabitethernet 0). The RSA keypair is named sshkeys.

This example only uses the commands required to configure persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
```

In the following example, a transport map is configured that will apply the following settings to any users attempting to access the Management Ethernet port via SSH:

- Users using SSH will wait for the vty line to become active, but will enter diagnostic mode if the attempt to access IOS through the vty line is interrupted.
- The RSA keypair name is "sshkeys"
- The connection allows one authentication retry.
- The banner "--Welcome to Diagnostic Mode--" will appear if diagnostic mode is entered as a result of SSH handling through this transport map.
- The banner "--Waiting for vty line--" will appear if the connection is waiting for the vty line to become active.

The transport map is then applied to the interface when the **transport type persistent ssh input** command is entered to enable persistent SSH.

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1


Router(config-tmap)# banner diagnostic X


Enter TEXT message.  End with the character 'X'.


--Welcome to Diagnostic Mode--


X


Router(config-tmap)#banner wait X
Enter TEXT message.  End with the character 'X'.
--Waiting for vty line--
X
Router(config-tmap)#
time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
```

```
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
```

# Viewing Console Port, SSH, and Telnet Handling Configurations

Use the **show transport-map all name** *transport-map-name* | **type console persistent ssh telnet**]]] EXEC or privileged EXEC command to view the transport map configurations.

In the following example, a console port, persistent SSH, and persistent Telnet transport are configured on the router and various forms of the **show transport-map** command are entered to illustrate the various ways the **show transport-map** command can be entered to gather transport map configuration information.

```
Router# show transport-map all
Transport Map:
  Name: consolehandler
  Type: Console Transport
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for the IOS CLI
  bshell banner:
Welcome to Diagnostic Mode
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS prompt
  Bshell banner:

Welcome to Diagnostic Mode
SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys
Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS process
  Bshell banner:
Welcome to Diagnostic Mode
Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport
Connection:
  Wait option: Wait Allow
Router# show transport-map type console
Transport Map:
  Name: consolehandler
  Type: Console Transport
Connection:
  Wait option: Wait Allow Interruptable
```

```
  Wait banner:
Waiting for the IOS CLI
  Bshell banner:
Welcome to Diagnostic Mode
Router# show transport-map type persistent ssh
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS prompt
  Bshell banner:
Welcome to Diagnostic Mode
SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys
Router# show transport-map type persistent telnet

Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS process
  Bshell banner:
Welcome to Diagnostic Mode
Transport Map:
  Name: telnethandling1
  Type: Persistent Telnet Transport
Connection:
  Wait option: Wait Allow
Router# show transport-map name telnethandler
Transport Map:
  Name: telnethandler
  Type: Persistent Telnet Transport
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS process
  Bshell banner:
Welcome to Diagnostic Mode
Router# show transport-map name consolehandler
Transport Map:
  Name: consolehandler
  Type: Console Transport
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for the IOS CLI
  Bshell banner:
Welcome to Diagnostic Mode
Router# show transport-map name sshhandler
Transport Map:
  Name: sshhandler
  Type: Persistent SSH Transport
```

```
Interface:
  GigabitEthernet0
Connection:
  Wait option: Wait Allow Interruptable
  Wait banner:
Waiting for IOS prompt
  Bshell banner:
Welcome to Diagnostic Mode
SSH:
  Timeout: 120
  Authentication retries: 5
  RSA keypair: sshkeys
Router#
```

The **show platform software configuration access policy** command can be used to view the current configurations for the handling of incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection, as well as any information on the currently configured banners. Unlike **show transport-map**, this command is available in diagnostic mode so it can be entered in cases when you need transport map configuration information but cannot access the IOS CLI.

```
Router# show platform software configuration access policy
The current access-policies
Method      : telnet
Rule        : wait
Shell banner:
Wait banner :
Method      : ssh
Rule        : wait
Shell banner:
Wait banner :
Method      : console
Rule        : wait with interrupt
Shell banner:
Wait banner :
```

In the following example, the connection policy and banners are set for a persistent SSH transport map, and the transport map is enabled.

The **show platform software configuration access policy** output is given both before the new transport map is enabled and after the transport map is enabled so the changes to the SSH configuration are illustrated in the output.

```
Router# show platform software configuration access policy

The current access-policies
Method      : telnet
Rule        : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode
Wait banner :
Waiting for IOS Process
Method      : ssh
Rule        : wait
Shell banner:
Wait banner :
Method      : console
Rule        : wait with interrupt
Shell banner:
Wait banner :
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message.  End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message.  End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
Router(config)# exit
Router# show platform software configuration access policy
The current access-policies
Method      : telnet
Rule        : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode
Wait banner :
Waiting for IOS process
Method      : ssh
Rule        : wait with interrupt
Shell banner:
Welcome to Diag Mode
Wait banner :
Waiting for IOS
Method      : console
Rule        : wait with interrupt
Shell banner:
Wait banner :
```

CHAPTER 4

# Configuring Clocking and Timing

This chapter explains how to configure timing ports on the Route Switch Processor (RSP) modules and includes the following sections:



# Clocking and Timing Restrictions

The following clocking and timing restrictions apply to the chassis:

- Interfaces carrying PTP traffic must be under the same VPN Routing and Forwarding (VRF). Misconfiguration will cause PTP packet loss.

  Use the 10 Gigabit Links to configure VRF on two Cisco RSP3 Routers.

- You can configure only a single clocking input source within each group of eight ports (0–7 and 8–15) on the T1/E1 interface module using the **network-clock input-source** command.
- Multicast timing is *not* supported.
- Out-of-band clocking and the **recovered-clock** command are *not* supported.
- Precision Time Protocol (PTP) is supported only on loopback interfaces.
- Synchronous Ethernet clock sources are *not* supported with PTP. Conversely, PTP clock sources are not supported with synchronous Ethernet except when configured as hybrid clock. However, you can use hybrid clocking to allow the chassis to obtain frequency using Synchronous Ethernet, and phase using PTP.
- Time of Day (ToD) and 1 Pulse per Second (1PPS) input is *not* supported when the chassis is in boundary clock mode.
- Multiple ToD clock sources are *not* supported.
- PTP redundancy is supported only on unicast negotiation mode; you can configure up to three server clocks in redundancy mode.

- In order to configure time of day input, you must configure both an input 10 Mhz and an input 1 PPS source.
- PTP over IPv6 is *not* supported.
- SyncE Rx and Tx is supported on uplink interfaces when using 8 x 1 GE Gigabit Ethernet SFP Interface Module.
- When PTP is configured, changing the configuration mode from LAN to WAN or WAN to LAN is *not* supported for following IMs:
    - 2x10G
    - 8x1G_1x10G_SFP
    - 8x1G_1x10G_CU
- PTP functionality is restricted by license type.

**Note** If you install the IEEE 1588-2008 BC/MC licenseIEEE 1588-2008 BC/MC license (available by default), you must reload the chassis to use the full PTP functionality.

**Note** By default, all timing licenses are already included on the Cisco NCS 4200 routers.

- End-to-end Transparent Clock is *not* supported for PTP over Ethernet.
- Transparent clock is not supported on the Cisco RSP3 Module.
- G.8265.1 telecom profiles are *not* supported with PTP over Ethernet.
- The chassis does *not* support a mix of IPv4 and Ethernet clock ports when acting as a transparent clock or boundary clock.

The following restrictions apply when configuring synchronous Ethernet SSM and ESMC:

- To use the **network-clock synchronization ssm option** command, ensure that the chassis configuration does *not* include the following:
    - Input clock source
    - Network clock quality level
    - Network clock source quality source (synchronous Ethernet interfaces)
- The **network-clock synchronization ssm option** command must be compatible with the **network-clock eec** command in the configuration.
- To use the **network-clock synchronization ssm option** command, ensure that there is *not* a network clocking configuration applied to synchronous Ethernet interfaces, BITS interfaces, and timing port interfaces.

- SSM and ESMC are SSO-coexistent, but not SSO-compliant. The chassis goes into hold-over mode during switchover and restarts clock selection when the switchover is complete.
- The chassis does not support ESMC messages on the S1 byte on SONET/SDH and T1/E1 interface modules.
- It is recommended that you do *not* configure multiple input sources with the same priority as this impacts the TSM (Switching message delay).
- You can configure a maximum of 4 clock sources on interface modules, with a maximum of 2 per interface module. This limitation applies to both synchronous Ethernet and TDM interfaces.
- When you configure the ports using the **synchronous mode** command on a copper interface, the port attempts to auto-negotiate with the peer-node copper port and hence the auto negotiation is incomplete as both the ports try to act as server clock, which in turn makes the port down. Hence, for a successful clock sync to happen, you should configure the ports using **network-clock input-source** *1* **interface** *interface id* command prior to the configuration using the **synchronous mode** command under the interfaces to ensure that one of the ports behaves as a server clock.

  It is not recommended to configure the copper ports using the **synchronous mode** command.

## Restrictions on RSP3 Module

The following clocking and timing restrictions are supported on the RSP3 Module:

- Precision Time Protocol (PTP) is supported only on the routed interfaces.
- Transparent Clock over 1 Gigabit Ethernet port performance is *not good.*
- PTP is supported for LAN for the following IMs. WAN is not supported.
  - 2x40
  - 1x100 GE
  - 8x10 GE
- To shift from non hybrid clock configuration to hybrid clock configuration, you must first unconfigure PTP, unconfigure netsync, reconfigure netsync and configure hybrid PTP.

# Clocking and Timing Overview

The chassis have the following timing ports:

- 1 PPS Input/Output
- 10 Mhz Input/Output
- ToD
- Building Integrated Timing Supply (BITS)

You can use the timing ports on the chassis to perform the following tasks:

- Provide or receive 1 PPS messages
- Provide or receive time of day (ToD) messages

- Provide output clocking at 10 Mhz, 2.048 Mhz, and 1.544 Mhz
- Receive input clocking at 10 Mhz, 2.048 Mhz, and 1.544 Mhz

**Note** Timing input and output is handled by the active RSP.

**Note** For timing redundancy, you can use a Y cable to connect a GPS timing source to multiple RSPs. For information, see the *Cisco NCS 4206 Series Hardware Installation Guide*.

SyncE is supported in both LAN and WAN mode on a 10 Gigabit Ethernet interface.

The following sections describe how to configure clocking and timing features on the chassis.

# Understanding PTP

The Precision Time Protocol (PTP), as defined in the IEEE 1588 standard, synchronizes with nanosecond accuracy the real-time clocks of the devices in a network. The clocks in are organized into a server-member hierarchy. PTP identifies the switch port that is connected to a device with the most precise clock. This clock is referred to as the server clock. All the other devices on the network synchronize their clocks with the server and are referred to as members. Constantly exchanged timing messages ensure continued synchronization.

PTP is particularly useful for industrial automation systems and process control networks, where motion and precision control of instrumentation and test equipment are important.

***Table 6: Nodes within a PTP Network***

| Network Element | Description |
|---|---|
| Grandmaster (GM) | A network device physically attached to the server time source. All clocks are synchronized to the grandmaster clock. |
| Ordinary Clock (OC) | An ordinary clock is a 1588 clock with a single PTP port that can operate in one of the following modes:<br>• Server mode—Distributes timing information over the network to one or more client clocks, thus allowing the client to synchronize its clock to the server.<br>• Client mode—Synchronizes its clock to a server clock. You can enable the client mode on up to two interfaces simultaneously in order to connect to two different server clocks. |
| Boundary Clock (BC) | The device participates in selecting the best server clock and can act as the server clock if no better clocks are detected.<br>Boundary clock starts its own PTP session with a number of downstream clients. The boundary clock mitigates the number of network hops and results in packet delay variations in the packet network between the Grandmaster and Client clock. |
| Transparent Clock (TC) | A transparent clock is a device or a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of time calculations. |

## Telecom Profiles

Cisco IOS XE Release 3.8 introduces support for telecom profiles, which allow you to configure a clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes. For information about how to configure telecom profiles, see Configuring Clocking and Timing, on page 47.

Effective Cisco IOS-XE Release 3.18, the G.8275.1 telecom profile is also supported on the Cisco NCS 4206 Series with RSP2 module. For more information, see G.8275.1 Telecom Profile .

## PTP Redundancy

PTP redundancy is an implementation on different clock nodes. This helps the PTP subordinate clock node achieve the following:

- Interact with multiple primary ports such as grand primary clocks and boundary clock nodes.
- Open PTP sessions.
- Select the best primary from the existing list of primary clocks (referred to as the primary PTP primary port or primary clock source).
- Switch to the next best primary available in case the primary primary fails, or the connectivity to the primary primary fails.

**Note** The Cisco NCS 4206 Series chassis supports unicast-based timing as specified in the 1588-2008 standard.

For instructions on how to configure PTP redundancy, see Configuring PTP Redundancy, on page 67.

## PTP Asymmetry Readjustment

Each PTP node can introduce delay asymmetry that affects the adequate time and phase accuracy over the networks. Asymmetry in a network occurs when one-way-delay of forward path (also referred as forward path delay or ingress delay) and reverse path (referred as reverse path delay or egress delay) is different. The magnitude of asymmetry can be either positive or negative depending on the difference of the forward and reverse path delays.

Effective Cisco IOS XE Gibraltar 16.10.1, PTP asymmetry readjustment can be performed on each PTP node to compensate for the delay in the network.

### Restriction

In default profile configuration, delay-asymmetry value is provided along with the clock source command. This restricts it to change the delay-asymmetry value with a complete reconfiguration of **clock source** command. The delay-asymmetry value should be considered as static and cannot be changed at run-time.

## PTP Redundancy Using Hop-By-Hop Topology Design

Real world deployments for IEEE-1588v2 for mobile backhaul requires the network elements to provide synchronization and phase accuracy over IP or MPLS networks along with redundancy.

In a ring topology, a ring of PTP boundary clock nodes are provisioned such that each boundary clock node provides synchronization to a number of PTP client clocks connected to it. Each such ring includes at least two PTP server clocks with a PRC traceable clock.

However, with this topology the following issues may occur:

- Node asymmetry and delay variation—In a ring topology, each boundary clock uses the same server, and the PTP traffic is forwarded through intermediate boundary clock nodes. As intermediate nodes do not correct the timestamps, variable delay and asymmetry for PTP are introduced based on the other traffic passing through such nodes, thereby leading to incorrect results.
- Clock redundancy—Clock redundancy provides redundant network path when a node goes down. In a ring topology with PTP, for each unicast PTP solution, the roles of each node is configured. The PTP clock path may not be able to reverse without causing timing loops in the ring.

### No On-Path Support Topology

The topology (see Figure 1: Deployment in a Ring - No On-Path Support with IPv4, on page 38) describes a ring with no on-path support. S1 to S5 are the boundary clocks that use the same server clocks. GM1 and GM2 are the grandmaster clocks. In this design, the following issues are observed:

- Timestamps are not corrected by the intermediate nodes.
- Difficult to configure the reverse clocking path for redundancy.
- Formation of timings loops.

*Figure 1: Deployment in a Ring - No On-Path Support with IPv4*

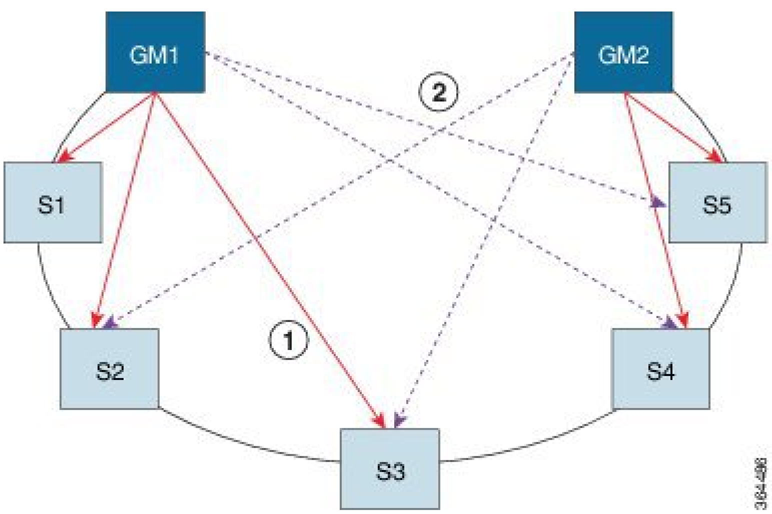



*Table 7: PTP Ring Topology—No On-Path Support*

| Clock Nodes | Behavior in the PTP Ring |
|---|---|
| GM1 | Grandmaster Clock |
| GM2 | Grandmaster Clock |
| S1 | Server Clocks: M1 (1st), M2 (2nd) |

| Clock Nodes | Behavior in the PTP Ring |
|---|---|
| S2 | Server Clocks: M1 (1st), M2 (2nd) |
| S3 | Server Clocks: M1 (1st), M2 (2nd) |
| S4 | Server Clocks: M2 (1st), M1 (2nd) |
| S5 | Server Clocks: M2 (1st), M1 (2nd) |

A solution to the above issue is addressed by using Hop-by-Hop topology configuration.

## Hop-By-Hop Topology in a PTP Ring

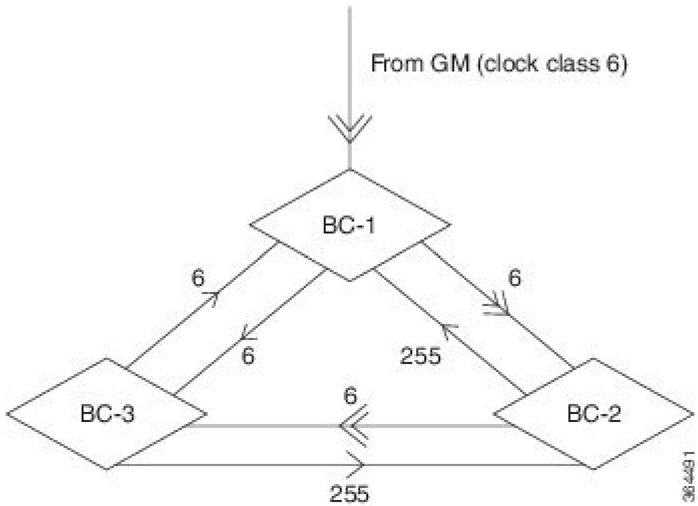
PTP Ring topology is designed by using Hop-By-Hop configuration of PTP boundary clocks. In this topology, each BC selects its adjacent nodes as PTP Server clocks, instead of using the same GM as the PTP server. These PTP BC server clocks are traceable to the GM in the network. Timing loop are not formed between adjacent BC nodes. The hot Standby BMCA configuration is used for switching to next the best server during failure.

### Prerequisites

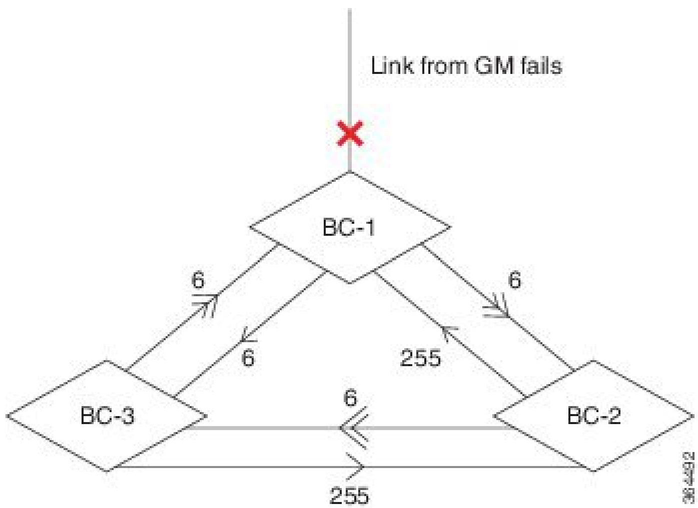
- PTP boundary clock configuration is required on all clock nodes in the ring, except the server clock nodes (GM), which provide the clock timing to ring. In the above example (see Figure 5-1) nodes S1 ... S5 must be configured as BC.
- The server clock (GM1 and GM2 in Figure 5-1) nodes in the ring can be either a OC server or BC server.
- Instead of each BC using same the GM as a PTP server, each BC selects its adjacent nodes as PTP server clocks. These PTP BC-server clocks are traceable to the GM in the network.
- Boundary clock nodes must be configured with the **single-hop** keyword in the PTP configuration to ensure that a PTP node can communicate with it’s adjacent nodes only.

### Restrictions

- Timing loops should not exist in the topology. For example, if for a node there are two paths to get the same clock back, then the topology is not valid. Consider the following topology and configuration.




The paths with double arrows (>>) are the currently active clock paths and paths with single arrow (>) are redundant clock path. This configuration results in a timing loop if the link between the BC-1 and GM fails.




- In a BC configuration, the same loopback interface should never be used for both Server and Client port configuration.
- **Single-hop** keyword is not supported for PTP over MPLS with explicit null configuration. The Single-hop keyword is not supported when PTP packets are sent out with a MPLS tag.

### On-Path Support Topology Scenario

Consider the topology as shown in Figure 5-1.

*Figure 2: PTP Ring Topology—On-Path Support*

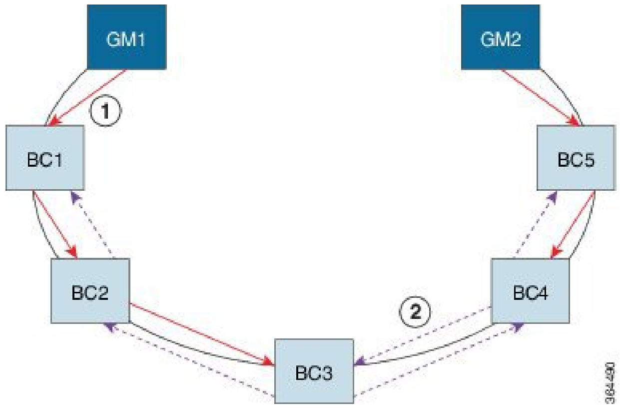



*Table 8: PTP Ring Topology—On-Path Support*

| Clock Node | Behavior in the PTP Ring |
|---|---|
| GM1 | Grandmaster Clock |
| GM2 | Grandmaster Clock |
| BC1 | Server Clocks: M1 (1st), BC2 (2nd)<br>Client Clocks: BC2 |
| BC2 | Server Clocks: BC1(1st), BC3 (2nd)<br>Client Clocks: BC1, BC3 |
| BC3 | Server Clocks: BC2 (1st), BC4 (2nd)<br>Client Clocks: BC2, BC4 |
| BC4 | Server Clocks: BC5 (1st), BC3 (2nd)<br>Client Clocks: BC3, BC5 |
| BC5 | Server Clocks: M2(1st), BC4 (2nd)<br>Client Clocks: BC4 |

Now consider there is a failure between BC1 and BC2 (see Figure 5-3). In this case, the BC2 cannot communicate with GM1. Node BC2 receives the clock from BC3, which in turn receives the clock from GM2.

*Figure 3: Deployment in a Ring—On-Path Support (Failure)*

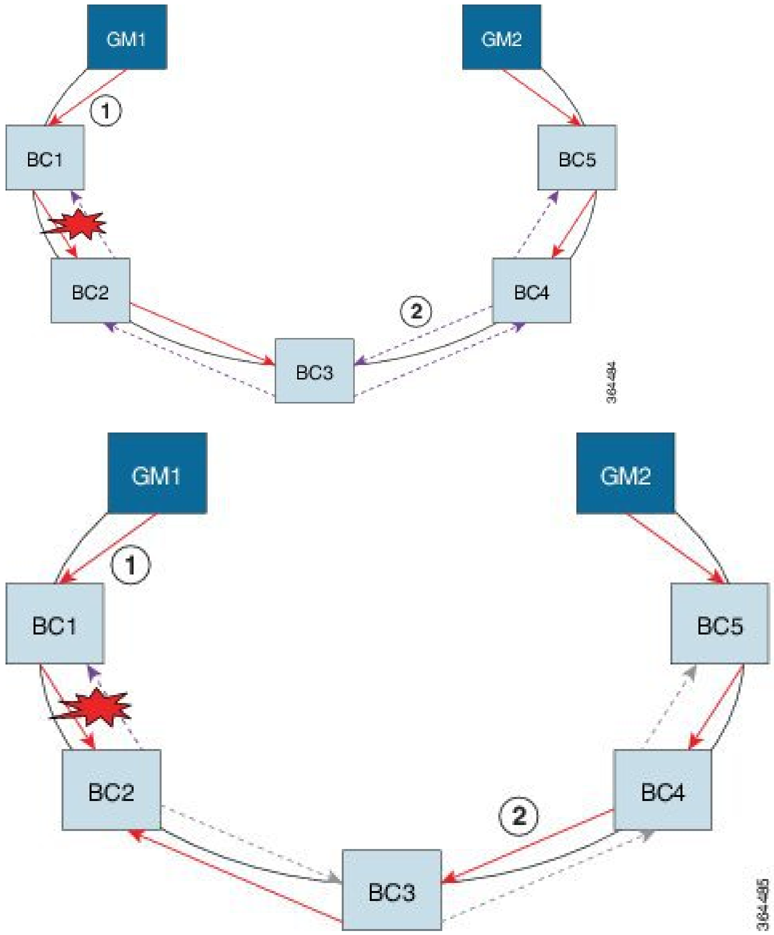



*Table 9: PTP Ring Topology—On-Path Support (Failure)*

| Clock Node | Behavior in the PTP Ring[3] |
|---|---|
| GM1 | Grandmaster Clock |
| GM2 | Grandmaster Clock |
| BC1 | Server Clocks: M1 (1st), BC2 (2nd)<br>Client Clocks: BC2 |
| BC2 | Server Clocks: BC1(1st), BC3 (2nd)<br>Client Clocks: BC1, BC3 |
| BC3 | Server Clocks: BC2 (1st), BC4 (2nd)<br>Client Clocks: BC2, BC4 |
| BC4 | Server Clocks: BC5 (1st), BC3 (2nd)<br>Client Clocks: BC3, BC5 |

| Clock Node | Behavior in the PTP Ring[3] |
|---|---|
| BC5 | Server Clocks: M2(1st), BC4 (2nd)<br>Client Clocks: BC4 |

3 Red indicates that GM is not traceable and there is no path to the client.

### Configuration Example

PTP Ring boundary clocks must be configured with **single-hop** keyword in PTP configuration. The PTP node can communicate with its adjacent nodes only. This is required for PTP hop-by-hop ring topology.

```
ptp clock boundary domain 0
           clock-port client-port slave
               transport ipv4 unicast interface Lo0 negotiation single-hop
               clock source 1.1.1.1
               clock source 2.2.2.2 1
           clock-port server-port master
               transport ipv4 unicast interface Lo1 negotiation single-hop
.
.
```

**Note** The **single-hop** keyword is not supported for PTP over MPLS with explicit NULL configurations. The **single-hop** keyword is not supported when PTP packets are sent out with a MPLS tag.

For information on configuring PTP redundancy, see Configuring PTP Redundancy, on page 67.

## BMCA

Starting Cisco IOS XE Release 3.15, BMCA is supported on the chassis.

The BMCA is used to select the server clock on each link, and ultimately, select the grandmaster clock for the entire Precision Time Protocol (PTP) domain. BCMA runs locally on each port of the ordinary and boundary clocks, and selects the best clock.

The best server clock is selected based on the following parameters:

- Priority—User-configurable value ranging from 0 to 255; lower value takes precedence
- Clock Class—Defines the traceability of time or frequency from the grandmaster clock
- Alarm Status—Defines the alarm status of a clock; lower value takes precedence

By changing the user-configurable values, network administrators can influence the way the grandmaster clock is selected.

BMCA provides the mechanism that allows all PTP clocks to dynamically select the best server clock (grandmaster) in an administration-free, fault-tolerant way, especially when the grandmaster clocks changes.

For information on configuring BMCA, see Configuring an Ordinary Clock, on page 47 and Configuring a Boundary Clock, on page 55.

### Hybrid BMCA

In hybrid BMCA implementation, the phase is derived from a PTP source and frequency is derived from a physical lock source. More than one server clock is configured in this model and the best server clock is selected. If the physical clock goes down, then PTP is affected.

#### Configuration Example

#### Hybrid BMCA on Ordinary Clock

```
ptp clock ordinary domain 0 hybrid
 clock-port client-port slave
  transport ipv4 unicast interface Lo0 negotiation
  clock source 133.133.133.133
 clock source 144.144.144.144 1
 clock source 155.155.155.155 2

Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

#### Hybrid BMCA on Boundary Clock

```
ptp clock boundary domain 0 hybrid
 clock-port client-port slave
  transport ipv4 unicast interface Lo0 negotiation
  clock source 133.133.133.133
 clock source 144.144.144.144 1
 clock source 155.155.155.155 2
 clock-port server-port master
  transport ipv4 unicast interface Lo1 negotiation
Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

## Hybrid Clocking

The Cisco NCS 4206 Series Chassis support a hybrid clocking mode that uses clock frequency obtained from the synchronous Ethernet port while using the phase (ToD or 1 PPS) obtained using PTP. The combination of using physical source for frequency and PTP for time and phase improves the performance as opposed to using only PTP.

**Note** When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same server clock.

For more information on how to configure hybrid clocking, see Configuring a Hybrid Clock, on page 59.

## Transparent Clocking

A transparent clock is a network device such as a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of timing calculations. The transparent clock ports have no state because the transparent clock does not need to synchronize to the grandmaster clock.

There are two kinds of transparent clocks:

- End-to-end transparent clock—Measures the residence time of a PTP message and accumulates the times in the correction field of the PTP message or an associated follow-up message.

- Peer-to-peer transparent clock— Measures the residence time of a PTP message and computes the link delay between each port and a similarly equipped port on another node that shares the link. For a packet, this incoming link delay is added to the residence time in the correction field of the PTP message or an associated follow-up message.

**Note** The Cisco NCS 4206 Series Chassis does not currently support peer-to-peer transparent clock mode.

For information on how to configure the Cisco NCS 4206 Series Chassis as a transparent clock, see Configuring a Transparent Clock, on page 57.

## Time of Day (TOD)

You can use the time of day (ToD) and 1PPS ports on the Cisco NCS 4206 Series Chassis to exchange ToD clocking. In server mode, the chassis can receive time of day (ToD) clocking from an external GPS unit; the chassis requires a ToD, 1PPS, and 10MHZ connection to the GPS unit.

In client mode, the chassis can recover ToD from a PTP session and repeat the signal on ToD and 1PPS interfaces.

For instructions on how to configure ToD on the Cisco NCS 4206 Series Chassis, see the Configuring an Ordinary Clock, on page 47.

### Synchronizing the System Clock to Time of Day

You can set the chassis system time to synchronize with the time of day retrieved from an external GPS device. For information on how to configure this feature, see Synchronizing the System Time to a Time-of-Day Source, on page 72.

# Timing Port Specifications

The following sections provide specifications for the timing ports on the Cisco NCS 4206 Series Chassis.

## BITS Framing Support

The following table lists the supported framing modes for a BITS port.

*Table 10: Framing Modes for a BITS Port on a Cisco NCS 4206 Chassis*

| BITS or SSU Port Support Matrix | Framing Modes Supported | SSM or QL Support | Tx Port | Rx Port |
|---|---|---|---|---|
| T1 | T1 ESF | Yes | Yes | Yes |
| T1 | T1 SF | No | Yes | Yes |
| E1 | E1 CRC4 | Yes | Yes | Yes |
| E1 | E1 FAS | No | Yes | Yes |
| 2048 kHz | 2048 kHz | No | Yes | Yes |

The BITS port behaves similarly to the T1/E1 ports on the T1/E1 interface module; for more information about configuring T1/E1 interfaces, see the *Configuring T1/E1 Interfaces* document.

# Understanding Synchronous Ethernet ESMC and SSM

Synchronous Ethernet incorporates the Synchronization Status Message (SSM) used in Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) networks. While SONET and SDH transmit the SSM in a fixed location within the frame, Ethernet Synchronization Message Channel (ESMC) transmits the SSM using a protocol: the IEEE 802.3 Organization-Specific Slow Protocol (OSSP) standard.

The ESMC carries a Quality Level (QL) value identifying the clock quality of a given synchronous Ethernet timing source. Clock quality values help a synchronous Ethernet node derive timing from the most reliable source and prevent timing loops.

When configured to use synchronous Ethernet, the chassis synchronizes to the best available clock source. If no better clock sources are available, the chassis remains synchronized to the current clock source.

The chassis supports two clock selection modes: QL-enabled and QL-disabled. Each mode uses different criteria to select the best available clock source.

For more information about Ethernet ESMC and SSM, see Configuring Synchronous Ethernet ESMC and SSM, on page 74.

**Note** The chassis can only operate in one clock selection mode at a time.

**Note** PTP clock sources are not supported with synchronous Ethernet.

## Clock Selection Modes

The chassis supports two clock selection modes, which are described in the following sections.

### QL-Enabled Mode

In QL-enabled mode, the chassis considers the following parameters when selecting a clock source:

- Clock quality level (QL)
- Clock availability
- Priority

### QL-Disabled Mode

In QL-disabled mode, the chassis considers the following parameters when selecting a clock source:

- Clock availability
- Priority

**Note** You can use override the default clock selection using the commands described in the Managing Clock Source Selection, on page 78.

> **Note** 8275.1 profile does not support QL-disabled mode on RSP3.

## Managing Clock Selection

You can manage clock selection by changing the priority of the clock sources; you can also influence clock selection by modifying modify the following clock properties:

- Hold-Off Time: If a clock source goes down, the chassis waits for a specific hold-off time before removing the clock source from the clock selection process. By default, the value of hold-off time is 300 ms.
- Wait to Restore: The amount of time that the chassis waits before including a newly active synchronous Ethernet clock source in clock selection. The default value is 300 seconds.
- Force Switch: Forces a switch to a clock source regardless of clock availability or quality.
- Manual Switch: Manually selects a clock source, provided the clock source has a equal or higher quality level than the current source.

For more information about how to use these features, see Managing Clock Source Selection, on page 78.

# Configuring Clocking and Timing

The following sections describe how to configure clocking and timing features on the chassis:

## Configuring an Ordinary Clock

The following sections describe how to configure the chassis as an ordinary clock.

### Configuring a Server Ordinary Clock

Follow these steps to configure the chassis to act as a Server ordinary clock.

#### Procedure

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enters configuration mode.

**Step 3** **platformptp masterprtc-only-enable**

**Example:**

```
Router(config)# platform ptp master prtc-only-enable
```

(Optional) Enable port deletion of the server clock.

**Step 4** **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number*

**Example:**

```
Router(config)# ptp clock ordinary domain 0
```

**Example:**

```
Router(config-ptp-clk)#
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP Server or Client clocks downstream.
- e2e-transparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the accuracy of 1588 clock at client.

**Step 5** **priority1** *priorityvalue*

**Example:**

```
Router(config-ptp-clk)# priority1 priorityvalue
```

Sets the preference level for a clock. client devices use the priority1 value when selecting a server clock: a lower priority1 value indicates a preferred clock. The priority1 value is considered above all other clock attributes.

Valid values are from 0-255. The default value is 128.

**Step 6** **priority2** *priorityvalue*

**Example:**

```
Router(config-ptp-clk)# priority2 priorityvalue
```

Sets a secondary preference level for a clock. client devices use the priority2 value when selecting a server clock: a lower priority2 value indicates a preferred clock. The priority2 value is considered only when the chassis is unable to use priority1 and other clock attributes to select a clock.

Valid values are from 0-255. The default value is 128.

**Step 7** **utc-offset** *value* **leap-second** *"date time"* **offset** {**-1** | **1**}

**Example:**

```
Router(config-ptp-clk)# utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
```

(Optional) Starting with Cisco IOS-XE Release 3.18SP, the new utc-offset CLI is used to set the UTC offset value.

Valid values are from 0-255. The default value is 36.

(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure the current UTC offset, leap second event date and Offset value (+1 or -1). Leap second configuration will work only when the frequency source is locked and ToD was up before.

- *"date time"*—Leap second effective date in dd-mm-yyyy hh:mm:ss format.

**Step 8** input [1pps] {R0 | R1}

**Example:**

```
Router(config-ptp-clk)# input 1pps R0
```

Enables Precision Time Protocol input 1PPS using a 1PPS input port.

Use R0 or R1 to specify the active RSP slot.

**Step 9** **tod** {**R0** | **R1**} {**ubx** | **nmea** | **cisco** | **ntp** | **cmcc**}

**Example:**

```
Router(config-ptp-clk)# tod R0 ntp
```

Configures the time of day message format used by the ToD interface.

**Note** It is mandatory that when electrical ToD is used, the **utc-offset** command is configured before configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the server and client clocks.

**Note** The ToD port acts as an input port in case of server clock and as an output port in case of client clock.

**Step 10** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-clk)# clock-port server-port master
```

Defines a new clock port and sets the port to PTP Server or Client mode; in server mode, the port exchanges timing packets with PTP client devices.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 11** Do one of the following:

- **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]*
- **transport ethernet unicast** [**negotiation**]

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation
```

Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.

The **negotiation** keyword configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

**Step 12** exit

Exits clock-port configuration.

**Step 13** **network-clock synchronization automatic**

**Example:**

```
Router(config)# network-clock synchronization automatic
```

Enables automatic selection of a clock source.

**Note** This command must be configured before any input source.

**Step 14** **network-clock synchronization mode ql-enabled**

**Example:**

```
Router(config)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

**Note** This command is disabled by default.

**Step 15** Use one of the following options:

- **network-clock input-source** *priority* **controller** {**SONET** | **wanphy**}
- **network-clock input-source** *priority* external {**R0** | **R1**} [**10m** | **2m**]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**cas** {**120ohms** | **75ohms** | **crc4**}}]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**crc4** | **fas**] {**120ohms** | **75ohms**} {**linecode** {**ami** | **hdb3**}}
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**t1** {**d4** | **esf** | **sf**} {**linecode** {**ami** | **b8zs**}}]
- **network-clock input-source** *priority* **interface** *type/slot/port*

**Example:**

```
Router(config)# network-clock input-source 1 external R0 10m
```

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.

**Step 16** **clock destination** *source-address* | *mac-address* {**bridge-domain** *bridge-domain-id}* | **interface** *interface-name*}

**Example:**

```
Router(config-ptp-port)# clock-source 8.8.8.1
```

Specifies the IP address or MAC address of a clock destination when the chassis is in PTP server mode.

**Step 17** **sync interval** *interval*

**Example:**

```
Router(config-ptp-port)# sync interval -4
```

Specifies the interval used to send PTP synchronization messages. The intervals are set using log base 2 values, as follows:

- 1—1 packet every 2 seconds
- 0—1 packet every second
- -1—1 packet every 1/2 second, or 2 packets per second
- -2—1 packet every 1/4 second, or 4 packets per second
- -3—1 packet every 1/8 second, or 8 packets per second
- -4—1 packet every 1/16 seconds, or 16 packets per second.
- -5—1 packet every 1/32 seconds, or 32 packets per second.
- -6—1 packet every 1/64 seconds, or 64 packets per second.
- -7—1 packet every 1/128 seconds, or 128 packets per second.

**Step 18** **announce interval** *interval*

**Example:**

```
Router(config-ptp-port)# announce interval 2
```

Specifies the interval for PTP announce messages. The intervals are set using log base 2 values, as follows:

- 3—1 packet every 8 seconds
- 2—1 packet every 4 seconds
- 1—1 packet every 2 seconds
- 0—1 packet every second
- -1—1 packet every 1/2 second, or 2 packets per second
- -2—1 packet every 1/4 second, or 4 packets per second
- -3—1 packet every 1/8 second, or 8 packets per second

**Step 19** **end**

**Example:**

```
Router(config-ptp-port)# end
```

Exit configuration mode.

**Step 20** linecode {ami | b8zs | hdb3}

**Example:**

```
Router(config-controller)# linecode ami
```

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

### Example

The following example shows that the utc-offset is configured before configuring the ToD to avoid a delay of 37 seconds between the Server or Client clocks:

```
ptp clock ordinary domain 24

local-priority 1

priority2 128
utc-offset 37
tod R0 cisco
clock-port server-port-1 master profile g8275.1 local-priority 1
transport ethernet multicast interface Gig 0/0/1
```

## Configuring a Client Ordinary Clock

Follow these steps to configure the chassis to act as a client ordinary clock.

### Procedure

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

**Example:**

```
Router(config)# ptp clock ordinary domain 0
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

**Step 4** **output [1pps] {R0 | R1}** [**offset** *offset-value*] [**pulse-width** *value*]

**Example:**

```
Router(config-ptp-clk)# output 1pps R0 offset 200 pulse-width 20 µsec
```

Enables Precision Time Protocol input 1PPS using a 1PPS input port.

Use R0 or R1 to specify the active RSP slot.

**Note** Effective Cisco IOS XE Everest 16.6.1, the 1pps pulse bandwith can be changed from the default value of 500 milliseconds to up to 20 microseconds.

**Step 5** **tod** {**R0 | R1}** {**ubx | nmea | cisco | ntp | cmcc**}

**Example:**

```
Router(config-ptp-clk)# tod R0 ntp
```

Configures the time of day message format used by the ToD interface.

**Note** The ToD port acts as an input port in case of server clock and as an output port in case of client clock.

**Step 6** **clock-port** *port-name* {**master | slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 7** Do one of the following:

- **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]*
- 
- **transport ethernet unicast** [**negotiation**]

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface loopback 0 negotiation
```

Specifies the transport mechanism for clocking traffic; you can use IPv4 or Ethernet transport.

The **negotiation** keyword configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

**Step 8** **clock source** *source-address* | *mac-address* {**bridge-domain** *bridge-domain-id*} | **interface** *interface-name*} [*priority*] [**delay-asymmetry** *delay asymmetry value* **nanoseconds**]

**Example:**

```
Router(config-ptp-port)# clock-source 8.8.8.1
```

Specifies the IP or MAC address of a PTP server clock.

- *priority*—Sets the preference level for a PTP clock.
- *delay asymmetry value*—Performs the PTP asymmetry readjustment on a PTP node to compensate for the delay in the network.

**Step 9** **announce timeout** *value*

**Example:**

```
Router(config-ptp-port)# announce timeout 8
```

Specifies the number of PTP announcement intervals before the session times out. Valid values are 1-10.

**Step 10** **delay-req interval** *interval*

**Example:**

```
Router(config-ptp-port)# delay-req interval 1
```

Configures the minimum interval allowed between PTP delay-request messages when the port is in the server state.

The intervals are set using log base 2 values, as follows:

- 3—1 packet every 8 seconds
- 2—1 packet every 4 seconds
- 1—1 packet every 2 seconds
- 0—1 packet every second
- -1—1 packet every 1/2 second, or 2 packets per second
- -2—1 packet every 1/4 second, or 4 packets per second
- -3—1 packet every 1/8 second, or 8 packets per second
- -4—1 packet every 1/16 seconds, or 16 packets per second.
- -5—1 packet every 1/32 seconds, or 32 packets per second.
- -6—1 packet every 1/64 seconds, or 64 packets per second.
- -7—1 packet every 1/128 seconds, or 128 packets per second.

**Step 11** **end**

**Example:**

```
Router(config-ptp-port)# end
```

Exit configuration mode.

**Step 12** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

# Configuring a Boundary Clock

Follow these steps to configure the chassis to act as a boundary clock.

**Procedure**

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **Router(config)# ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

**Example:**

```
Router(config)# ptp clock boundary domain 0
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP server to client clocks downstream.

- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

**Step 4** **time-properties persist** *value*

**Example:**

```
Router(config-ptp-clk)#
time-properties persist 600
```

(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure time properties holdover time. Valid values are from 0 to 10000 seconds. The default value is 300 seconds.

When a server clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged. In case leap second midnight occurs when holdover timer is running, utc-offset value is updated based on leap59 or leap61 flags. This value is used as long as there are no PTP packets being received from the selected server clock. In case the selected server clock is sending announce packets, the time-properties advertised by server clock is used.

**Step 5** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 6** **transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***]*

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```

Specifies the transport mechanism for clocking traffic.

The **negotiation** keyword configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

**Step 7** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.133
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

**Step 8** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-port)# clock-port server-port master
```

Sets the clock port to PTP Server or Client mode; in server mode, the port exchanges timing packets with PTP client devices.

**Note** The server clock-port does not establish a clocking session until the client clock-port is phase aligned.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 9** **transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***]*

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation
```

Specifies the transport mechanism for clocking traffic.

The **negotiation** keyword configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

**Step 10** **end**

**Example:**

```
Router(config-ptp-port)# end
```

Exit configuration mode.

**Step 11** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

### What to do next

# Configuring a Transparent Clock

Follow these steps to configure the chassis as an end-to-end transparent clock.

**Note** The Cisco NCS 4206 Series Chassis does not support peer-to-peer transparent clock mode.

**Note** The transparent clock ignores the domain number.

**Procedure**

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

**Example:**

```
Router(config)# ptp clock e2e-transparent domain 4
```

Configures the chassis as an end-to-end transparent clock.

**Step 4** **exit**

**Example:**

```
Router(config)# exit
```

Exit configuration mode.

**Step 5** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

# Configuring a Hybrid Clock

The following sections describe how to configure the chassis to act as a hybrid clock.

## Configuring a Hybrid Boundary Clock

Follow these steps to configure a hybrid clocking in boundary clock mode.

**Note** When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same server clock.

### Procedure

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **ptp clock** {**boundary**} **domain** *domain-number* [**hybrid**]

**Example:**

```
Router(config)# ptp clock boundary domain 0 hybrid
```

Configures the PTP clock. You can create the following clock types:

**Note** Hybrid mode is only supported with client clock-ports; server mode is not supported.

- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client downstream.

**Step 4** **time-properties persist** *value*

**Example:**

```
Router(config-ptp-clk)# time-properties persist 600
```

(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure time properties holdover time. Valid values are from 0 to 10000 seconds. The default value is 300 seconds.

When a server clock is lost, the time properties holdover timer starts. During this period, the time properties flags (currentUtcOffset, currentUtcOffsetValid, leap61, leap59) persist for the holdover timeout period. Once the holdover timer expires, currentUtcOffsetValid, leap59, and leap61 flags are set to false and the currentUtcOffset remains unchanged. In case leap second midnight occurs when holdover timer is running, utc-offset value is updated based on leap59 or leap61 flags. This value is used as long as there are no PTP packets being received from the selected server clock. In case the selected server clock is sending announce packets, the time-properties advertised by server is used.

**Step 5** **utc-offset** *value* **leap-second** *"date time"* **offset** {**-1** | **1**}

**Example:**

```
Router(config-ptp-clk)# utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
```

(Optional) Starting with Cisco IOS XE Release 3.18SP, the new utc-offset CLI is used to set the UTC offset value.

Valid values are from 0-255. The default value is 36.

(Optional) Starting with Cisco IOS-XE Release 3.18.1SP, you can configure the current UTC offset, leap second event date and Offset value (+1 or -1). Leap second configuration will work only when the frequency source is locked and ToD was up before.

- *"date time"*—Leap second effective date in dd-mm-yyyy hh:mm:ss format.

**Step 6** **min-clock-class***value*

**Example:**

```
Router(config-ptp-clk)# min-clock-class 157
```

Sets the threshold clock-class value. This allows the PTP algorithm to use the time stamps from a upstream server clock, only if the clock-class sent by the server clock is less than or equal to the configured threshold clock-class.

Valid values are from 0-255.

**Note** Min-clock-class value is supported only for PTP with single server clock source configuration.

**Step 7** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock.

**Note** Hybrid mode is only supported with client clock-ports; server mode is not supported.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 8** **transport ipv4** unicast **interface** *interface-type interface-number [***negotiationsingle-hop]**

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
or
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

**negotiation**—(Optional) configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

**single-hop**—(Optional)Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.

**Step 9** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.133
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

**Step 10** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-port)# clock-port server-port master
```

Sets the clock port to PTP server or client mode; in server mode, the port exchanges timing packets with PTP client devices.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 11** **transport ipv4** unicast **interface** *interface-type interface-number [***negotiation***] [***single-hop]**

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Lo1 negotiation
or
Router(config-ptp-port)# transport ipv4 unicast interface Lo1 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

**negotiation**—(Optional)configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

**single-hop**—(Optional) Must be configured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.

**Step 12** **exit**

Exit clock-port configuration.

**Step 13** **network-clock synchronization automatic**

**Example:**

```
Router(config)# network-clock synchronization automatic
```

Enables automatic selection of a clock source.

**Note** This command must be configured before any input source.

**Step 14** **network-clock synchronization mode ql-enabled**

**Example:**

```
Router(config)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

**Note** This command is disabled by default.

**Step 15** Use one of the following options:

- **network-clock input-source** *priority* **controller** {**SONET** | **wanphy**}
- **network-clock input-source** *priority* external {**R0** | **R1**} [**10m** | **2m**]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**cas** {**120ohms** | **75ohms** | **crc4**}}]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**crc4** | **fas**] {**120ohms** | **75ohms**} {**linecode** {**ami** | **hdb3**}}
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**t1** {**d4** | **esf** | **sf**} {**linecode** {**ami** | **b8zs**}}]
- **network-clock input-source** *priority* **interface** *type/slot/port*

**Example:**

```
Router(config)# network-clock input-source 1 external R0 10m
```

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.

**Step 16** **network-clock synchronization input-threshold** *ql value*

**Example:**

```
Router(config)# network-clock synchronization input-threshold <ql value>
```

(Optional) Starting with Cisco IOS-XE Release 3.18SP, this new CLI is used to set the threshold QL value for the input frequency source. The input frequency source, which is better than or equal to the configured threshold QL value, will be selected to recover the frequency. Otherwise, internal clock is selected.

**Step 17** **network-clock hold-off** {**0** | *milliseconds*}

**Example:**

```
Router(config)# network-clock hold-off 0
```

(Optional) Configures a global hold-off timer specifying the amount of time that the chassis waits when a synchronous Ethernet clock source fails before taking action.

**Note** You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.

For more information about this command, see Configuring Clocking and Timing, on page 33

**Step 18** **platformptpmasteralways-on**

**Example:**

```
Router(config)# platform ptp master always-on
```

(Optional) Keeps the server port up all the time. So, when the frequency source has acceptable QL, the egress packets are sent to the downstream clients even when the server port is not phase aligned.

**Step 19** **platformptphybrid-bcdownstream-enable**

**Example:**

```
Router(config)# platform ptp hybrid-bc downstream-enable
```

(Optional) Enables bust mode. When the difference between the forward timestamp of the previous packet and current packet is greater than 100ns, such timestamps are not provided to the APR. Due to this setting, the APR does not see unexpected and random time jumps in two sequential timestamps of the same PTP message-types. The same applies for the reverse path timestamps as well.

**Step 20** **end**

**Example:**

```
Router(config)# end
```

Exit configuration mode.

**Step 21** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

## Configuring a Hybrid Ordinary Clock

Follow these steps to configure a hybrid clocking in ordinary clock client mode.

**Note** When configuring a hybrid clock, ensure that the frequency and phase sources are traceable to the same server clock.

### Procedure

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

**Example:**

```
Router(config)# ptp clock ordinary domain 0 hybrid
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.

  **Note** Hybrid mode is only supported with client clock-ports; server mode is not supported.

- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

**Step 4** **output [1pps] {R0 | R1}** [**offset** *offset-value*] [**pulse-width** *value*]

**Example:**

```
Router(config-ptp-clk)# output 1pps R0 offset 200 pulse-width 20 µsec
```

Enables Precision Time Protocol input 1PPS using a 1PPS input port.

Use R0 or R1 to specify the active RSP slot.

**Note** Effective Cisco IOS XE Everest 16.6.1, the 1pps pulse bandwith can be changed from the default value of 500 milliseconds to up to 20 microseconds.

**Step 5** **tod** {**R0** | **R1}** {**ubx** | **nmea** | **cisco** | **ntp** | **cmcc**}

**Example:**

```
Router(config-ptp-clk)# tod R0 ntp
```

Configures the time of day message format used by the ToD interface.

**Note** The ToD port acts as an input port in case of server clock and as an output port in case of client clock.

**Step 6** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.

**Note** Hybrid mode is only supported with client clock-ports; server mode is not supported.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 7** **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***]*

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```

Specifies the transport mechanism for clocking traffic.

The **negotiation** keyword configures the router to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

**Step 8** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.133
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

**Step 9** **exit**

**Example:**

```
Router(config-ptp-port)# exit
```

Exit clock-port configuration.

**Step 10** **network-clock synchronization automatic**

**Example:**

```
Router(config-ptp-clk)# network-clock synchronization automatic
```

Enables automatic selection of a clock source.

**Note** This command must be configured before any input source.

**Step 11** **network-clock synchronization mode ql-enabled**

**Example:**

```
Router(config-ptp-clk)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

**Note** This command is disabled by default.

For more information about this command, see Configuring Clocking and Timing, on page 33

**Step 12** Use one of the following options:

- network-clock input-source <priority> controller {SONET | wanphy}
- network-clock input-source <priority> external {R0 | R1} [10m | 2m]
- network-clock input-source <priority> external {R0 | R1} [2048k | e1 {cas {120ohms | 75ohms | crc4}}]
- network-clock input-source <priority> external {R0 | R1} [2048k | e1 {crc4 | fas] {120ohms | 75ohms} {linecode {ami | hdb3}}
- network-clock input-source <priority> external {R0 | R1} [t1 {d4 | esf | sf} {linecode {ami | b8zs}}]
- network-clock input-source <priority> interface <type/slot/port>

**Example:**

```
Router(config)# network-clock input-source 1 external R0 10m
```

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.

**Step 13** **network-clock hold-off** {**0** | *milliseconds*}

**Example:**

```
Router(config-ptp-clk)# network-clock hold-off 0
```

(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

**Note** You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.

For more information about this command, see Configuring Clocking and Timing, on page 33

**Step 14** **end**

**Example:**

```
Router(config-ptp-clk)# end
```

Exit configuration mode.

**Step 15** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

# Configuring PTP Redundancy

The following sections describe how to configure PTP redundancy on the chassis:

## Configuring PTP Redundancy in Client Clock Mode

Follow these steps to configure clocking redundancy in client clock mode:

**Procedure**

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number* [**hybrid**]

**Example:**

```
Router(config#) ptp clock ordinary domain 0
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client clocks downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

**Step 4** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP server or client mode; in client mode, the port exchanges timing packets with a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 5** **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***] [***single-hop]**

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

- **negotiation**—(Optional) Configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

- **single-hop—**(Optional) **It ensures that the PTP node communicates only with the adjacent nodes.**

**Step 6** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.133 1
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

**Step 7** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.134 2
```

Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.

**Step 8** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.135
```

Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.

**Step 9** **end**

**Example:**

```
Router(config-ptp-port)# end
```

Exit configuration mode.

**Step 10** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

## Configuring PTP Redundancy in Boundary Clock Mode

Follow these steps to configure clocking redundancy in boundary clock mode:

**Procedure**

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **ptp clock** {**ordinary** | **boundary** | **e2e-transparent**} **domain** *domain-number*

**Example:**

```
Router(config)# ptp clock boundary domain 0
```

Configures the PTP clock. You can create the following clock types:

- ordinary—A 1588 clock with a single PTP port that can operate in Server or Client mode.
- boundary—Terminates PTP session from Grandmaster and acts as PTP Server to Client clocks downstream.
- e2e-ransparent—Updates the PTP time correction field to account for the delay in forwarding the traffic. This helps improve the acuracy of 1588 clock at client.

**Step 4** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-clk)# clock-port client-port slave
```

Sets the clock port to PTP Server or Client mode; in client mode, the port exchanges timing packets with a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 5** **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***] [***single-hop]**

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation
```

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 0 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

- **negotiation**—(Optional) Configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

- **single-hop—**(Optional) Must beconfigured, if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.

**Step 6** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.133 1
```

Specifies the address of a PTP server clock. You can specify a priority value as follows:

- No priority value—Assigns a priority value of 0.
- 1—Assigns a priority value of 1.
- 2—Assigns a priority value of 2, the highest priority.

**Step 7** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.134 2
```

Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.

**Step 8** **clock-source** *source-address [priority]*

**Example:**

```
Router(config-ptp-port)# clock source 133.133.133.135
```

Specifies the address of an additional PTP server clock; repeat this step for each additional server clock. You can configure up to three server clocks.

**Step 9** **clock-port** *port-name* {**master** | **slave**} [**profile** {**g8265.1**}]

**Example:**

```
Router(config-ptp-port)# clock-port server-port master
```

Specifies the address of a PTP server clock.

The **profile** keyword configures the clock to use the G.8265.1 recommendations for establishing PTP sessions, determining the best server clock, handling SSM, and mapping PTP classes.

**Note** Using a telecom profile requires that the clock have a domain number of 4–23.

**Step 10** **transport ipv4 unicast interface** *interface-type interface-number [***negotiation***] [***single-hop**]

**Example:**

```
Router(config-ptp-port)# transport ipv4 unicast interface Loopback 1 negotiation single-hop
```

Specifies the transport mechanism for clocking traffic.

- **negotiation**—(Optional) Configures the chassis to discover a PTP server clock from all available PTP clock sources.

**Note** PTP redundancy is supported only on unicast negotiation mode.

- **single-hop—**(Optional) Must be configured if Hop-by-Hop PTP ring topology is used. It ensures that the PTP node communicates only with the adjacent nodes.

**Step 11** **end**

**Example:**

```
Router(config-ptp-port)# end
```

Exit configuration mode.

**Step 12** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

# Synchronizing the System Time to a Time-of-Day Source

The following sections describe how to synchronize the system time to a time of day (ToD) clock source.

## Synchronizing the System Time to a Time-of-Day Source (Server Mode)

**Note** System time to a ToD source (Server Mode) can be configured only when PTP server is configured. See Configuring a Server Ordinary Clock, on page 47. Select any one of the four available ToD format; cisco, nmea, ntp or ubx.10m must be configured as network clock input source.

Follow these steps to configure the system clock to a ToD source in server mode.

### Procedure

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **tod-clock input-source** *priority* {**gps** {**R0** | **R1**} | **ptp domain** *domain*}

**Example:**

```
Router(config)# TOD-clock 2 gps R0/R1
```

In server mode, specify a GPS port connected to a ToD source.

**Step 4** **exit**

**Example:**

```
Router(config)# exit
```

Exit configuration mode.

**Step 5** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

## Synchronizing the System Time to a Time-of-Day Source (Client Mode)

**Note** System time to a ToD source (Client Mode) can be configured only when PTP client is configured. See Configuring a Client Ordinary Clock, on page 52.

Follow these steps to configure the system clock to a ToD source in client mode. In client mode, specify a PTP domain as a ToD input source.

### Procedure

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enter configuration mode.

**Step 3** **tod-clock input-source** *priority* {**gps** {**R0** | **R1**} | **ptp domain** *domain*}

**Example:**

```
Router(config)# TOD-clock 10 ptp domain 0
```

In client mode, specify a PTP domain as a ToD input source.

**Step 4** Router(config)# **end**

Exit configuration mode.

**Step 5** Router(config-controller)# linecode {ami | b8zs | hdb3}

Selects the linecode type.

- ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.
- b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for sonet controller only. This is the default for T1 lines.
- hdb3—Specifies high-density binary 3 (hdb3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines.

# Configuring Synchronous Ethernet ESMC and SSM

Synchronous Ethernet is an extension of Ethernet designed to provide the reliability found in traditional SONET/SDH and T1/E1 networks to Ethernet packet networks by incorporating clock synchronization features. The supports the Synchronization Status Message (SSM) and Ethernet Synchronization Message Channel (ESMC) for synchronous Ethernet clock synchronization.

The following sections describe ESMC and SSM support on the router.

## Configuring Synchronous Ethernet ESMC and SSM

Follow these steps to configure ESMC and SSM on the router.

**Procedure**

**Step 1** **enable**

**Example:**

```
Router> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

**Step 2** **configure terminal**

**Example:**

```
Router# configure terminal
```

Enters global configuration mode.

**Step 3** **network-clock synchronization automatic**

**Example:**

```
Router(config)# network-clock synchronization automatic
```

Enables the network clock selection algorithm. This command disables the Cisco-specific network clock process and turns on the G.781-based automatic clock selection process.

**Note** This command must be configured before any input source.

**Step 4** **network-clock eec** {**1** | **2**}

**Example:**

```
Router(config)# network-clock eec 1
```

Specifies the Ethernet Equipment Clock (EEC) type. Valid values are

- 1—ITU-T G.8262 option 1 (2048)
- 2—ITU-T G.8262 option 2 and Telcordia GR-1244 (1544)

**Step 5** **network-clock synchronization ssm option** {**1** | **2** {**GEN1** | **GEN2**}}

**Example:**

```
Router(config)# network-clock synchronization ssm option 2 GEN2
```

Configures the G.781 synchronization option used to send synchronization messages. The following guidelines apply for this command:

- Option 1 refers to G.781 synchronization option 1, which is designed for Europe. This is the default value.
- Option 2 refers to G.781 synchronization option 2, which is designed for the United States.
- GEN1 specifies option 2 Generation 1 synchronization.
- GEN2 specifies option 2 Generation 2 synchronization.

**Step 6** Use one of the following options:

- **network-clock input-source** *priority* **controller** {**SONET** | **wanphy**}
- **network-clock input-source** *priority* external {**R0** | **R1**} [**10m** | **2m**]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**cas** {**120ohms** | **75ohms** | **crc4**}}]
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**2048k** | **e1** {**crc4** | **fas**] {**120ohms** | **75ohms**} {**linecode** {**ami** | **hdb3**}}
- **network-clock input-source** *priority* **external** {**R0** | **R1**} [**t1** {**d4** | **esf** | **sf**} {**linecode** {**ami** | **b8zs**}}]
- **network-clock input-source** *priority* **interface** *type/slot/port*

**Example:**

```
Router(config)# network-clock input-source 1 external R0 10m
```

- (Optional) To nominate SDH or SONET controller as network clock input source.
- (Optional) To nominate 10Mhz port as network clock input source.
- (Optional) To nominate BITS port as network clock input source in e1 mode.
- (Optional) To nominate BITS port as network clock input source in e1 mode.

- (Optional) To nominate BITS port as network clock input source in t1 mode.
- (Optional) To nominate Ethernet interface as network clock input source.
- (Optional) To nominate PTP as network clock input source.

**Step 7** **network-clock synchronization mode ql-enabled**

**Example:**

```
Router(config)# network-clock synchronization mode ql-enabled
```

Enables automatic selection of a clock source based on quality level (QL).

**Note** This command is disabled by default.

**Step 8** **network-clock hold-off** {**0** | *milliseconds*}

**Example:**

```
Router(config)# network-clock hold-off 0
```

(Optional) Configures a global hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

**Note** You can also specify a hold-off value for an individual interface using the **network-clock hold-off** command in interface mode.

**Step 9** **network-clock wait-to-restore** *seconds*

**Example:**

```
Router(config)# network-clock wait-to-restore 70
```

(Optional) Configures a global wait-to-restore timer for synchronous Ethernet clock sources. The timer specifies how long the router waits before including a restored clock source in the clock selection process.

Valid values are 0 to 86400 seconds. The default value is 300 seconds.

**Note** You can also specify a wait-to-restore value for an individual interface using the **network-clock wait-to-restore** command in interface mode.

**Step 10** **network-clock revertive**

**Example:**

```
Router(config)# network-clock revertive
```

(Optional) Sets the router in revertive switching mode when recovering from a failure. To disable revertive mode, use the **no** form of this command.

**Step 11** **esmc process**

**Example:**

```
Router(config)# esmc process
```

Enables the ESMC process globally.

**Step 12** **network-clock external** *slot/card/port* **hold-off** {**0** | *milliseconds*}

**Example:**

```
Router(config)# network-clock external 0/1/0 hold-off 0
```

Overrides the hold-off timer value for the external interface.

**Step 13** **network-clock quality-level** {**tx** | **rx**} *value* {**controller** [**E1**| **BITS**] *slot/card/port* | external [**2m** | **10m** | **2048k** | **t1** | **e1**] }

**Example:**

```
Router(config)# network-clock quality-level rx qL-pRC external R0 e1 cas crc4
```

Specifies a quality level for a line or external clock source.

The available quality values depend on the G.781 synchronization settings specified by the **network-clock synchronization ssm option** command:

- Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.
- Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.
- Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.

**Step 14** **interface** *type number*

**Example:**

```
Router(config)# interface GigabitEthernet 0/0/1
```

**Example:**

```
Router(config-if)#
```

Enters interface configuration mode.

**Step 15** **synchronous mode**

**Example:**

```
Router(config-if)# synchronous mode
```

Configures the Ethernet interface to synchronous mode and automatically enables the ESMC and QL process on the interface.

**Step 16** network-clock source quality-level *value* {**tx** | **rx**}

**Example:**

```
Router(config-if)# network-clock source quality-level QL-PrC tx
```

Applies quality level on sync E interface.

The available quality values depend on the G.781 synchronization settings specified by the **network-clock synchronization ssm option** command:

- Option 1—Available values are QL-PRC, QL-SSU-A, QL-SSU-B, QL-SEC, and QL-DNU.
- Option 2, GEN1—Available values are QL-PRS, QL-STU, QL-ST2, QL-SMC, QL-ST4, and QL-DUS.
- Option 2, GEN 2—Available values are QL-PRS, QL-STU, QL-ST2, QL-TNC, QL-ST3, QL-SMC, QL-ST4, and QL-DUS.

**Step 17** **esmc mode** [**ql-disabled** | **tx** | **rx**] *value*

**Example:**

```
Router(config-if)# esmc mode rx QL-STU
```

Enables the ESMC process at the interface level. The **no** form of the command disables the ESMC process.

**Step 18** **network-clock hold-off** {*0* | *milliseconds*}

**Example:**

```
Router(config-if)# network-clock hold-off 0
```

(Optional) Configures an interface-specific hold-off timer specifying the amount of time that the router waits when a synchronous Ethernet clock source fails before taking action.

You can configure the hold-off time to either 0 or any value between 50 to 10000 ms. The default value is 300 ms.

**Step 19** **network-clock wait-to-restore** *seconds*

**Example:**

```
Router(config-if)# network-clock wait-to-restore 70
```

(Optional) Configures the wait-to-restore timer for an individual synchronous Ethernet interface.

**Step 20** **end**

**Example:**

```
Router(config-if)# end
```

Exits interface configuration mode and returns to privileged EXEC mode.

---

#### What to do next

You can use the **show network-clocks** command to verify your configuration.

## Managing Clock Source Selection

The following sections describe how to manage the selection on the chassis:

### Specifying a Clock Source

The following sections describe how to specify a synchronous Ethernet clock source during the clock selection process:

#### Selecting a Specific Clock Source

To select a specific interface as a synchronous Ethernet clock source, use the network-clock switch manual command in global configuration mode.

**Note** The new clock source must be of higher quality than the current clock source; otherwise the chassis does not select the new clock source.

| Command | Purpose |
|---|---|
| **network-clock switch manual external R0** \| **R1** {{**E1** {**crc4** \| **cas** \|**fas**}} {**T1** {**d4** \| **sf** \| **esf**}} } <br><br> `Router# network-clock switch manual external r0 e1 crc4` | Manually selects a synchronization source, provided the source is available and is within the range. |
| **network-clock clear switch** {**t0** \| **external** *slot/card/port* [**10m** \| **2m**]} <br><br> `Router# network-clock clear switch t0` | Disable a clock source selection. |

### Forcing a Clock Source Selection

To force the chassis to use a specific synchronous Ethernet clock source, use the **network-clock switch force** command in global configuration mode.

**Note** This command selects the new clock regardless of availability or quality.

**Note** Forcing a clock source selection overrides a clock selection using the **network-clock switch manual command.**

| Command | Purpose |
|---|---|
| **network-clock switch force external R0** \| **R1** {{**E1** {**crc4** \| **cas** \|**fas**}} {**T1** {**d4** \| **sf** \| **esf**}} } <br><br> `Router# network-clock switch force r0 e1 crc4` | Forces the chassis to use a specific synchronous Ethernet clock source, regardless of clock quality or availability. |
| **network-clock clear switch** {**t0** \| **external** *slot/card/port* [**10m** \| **2m**]} <br><br> `Router# network-clock clear switch t0` | Disable a clock source selection. |

### Disabling Clock Source Specification Commands

To disable a **network-clock switch manual** or **network-clock switch force** configuration and revert to the default clock source selection process, use the **network-clock clear switch** command.

| Command | Purpose |
|---|---|
| **network-clock clear switch** {**t0** \| **external** *slot/card/port* [**10m** \| **2m**]} <br><br> `Router# network-clock clear switch t0` | Disable a clock source selection. |

### Disabling a Clock Source

The following sections describe how to manage the synchronous Ethernet clock sources that are available for clock selection:

#### Locking Out a Clock Source

To prevent the chassis from selecting a specific synchronous Ethernet clock source, use the network-clock set lockout command in global configuration mode.

| Command | Purpose |
|---|---|
| **network-clock set lockout** {**interface** *interface_name slot/card/port* \| **external** {**R0** \| **R1** [ { **t1** {**sf** \| **esf** } **linecode** {**ami** \| **b8zs**}} \| **e1** [**crc4** \| **fas**] **linecode** [**hdb3** \| **ami**]} <br><br> `Router# network-clock set lockout interface GigabitEthernet 0/0/0` | Prevents the chassis from selecting a specific synchronous Ethernet clock source. |
| **network-clock clear lockout** {**interface** *interface_name slot/card/port* \| **external** {**R0** \| **R1** [ { **t1** {**sf** \| **esf** } **linecode** {**ami** \| **b8zs**}} \| **e1** [**crc4** \| **fas**] **linecode** [**hdb3** \| **ami**] } <br><br> `Router# network-clock clear lockout interface GigabitEthernet 0/0/0` | Disable a lockout configuration on a synchronous Ethernet clock source. |

#### Restoring a Clock Source

To restore a clock in a lockout condition to the pool of available clock sources, use the **network-clock clear lockout** command in global configuration mode.

| Command | Purpose |
|---|---|
| **network-clock clear lockout** {**interface** *interface_name slot/card/port* \| **external external** {**R0** \| **R1** [ { **t1** {**sf** \| **esf** } **linecode** {**ami** \| **b8zs**}} \| **e1** [**crc4** \| **fas**] **linecode** [**hdb3** \| **ami**] } <br><br> `Router# network-clock clear lockout interface GigabitEthernet 0/0/0` | Forces the chassis to use a specific synchronous Ethernet clock source, regardless of clock quality or availability. |

# Verifying the Configuration

You can use the following commands to verify a clocking configuration:

- show esmc—Displays the ESMC configuration.
- **show esmc detail**—Displays the details of the ESMC parameters at the global and interface levels.
- show network-clock synchronization—Displays the chassis clock synchronization state.

- show network-clock synchronization detail—Displays the details of network clock synchronization parameters at the global and interface levels.
- **show ptp clock dataset**
- **show ptp port dataset**
- **show ptp clock running**
- **show platform software ptpd statistics**
- **show platform ptp all**
- **show platform ptp tod all**

# Troubleshooting

Table 11: SyncE Debug Commands , on page 81 list the debug commands that are available for troubleshooting the SyncE configuration on the chassis:

**Caution** We recommend that you do not use **debug** commands without TAC supervision.

*Table 11: SyncE Debug Commands*

| Debug Command | Purpose |
|---|---|
| **debug platform network-clock** | Debugs issues related to the network clock including active-standby selection, alarms, and OOR messages. |
| **debug network-clock** | Debugs issues related to network clock selection. |
| **debug esmc error**<br>**debug esmc event**<br>debug esmc packet [interface *interface-name*]<br>debug esmc packet rx [interface *interface-name*]<br>debug esmc packet tx [interface *interface-name*] | These commands verify whether the ESMC packets are transmitted and received with proper quality-level values. |

Table 12: Troubleshooting Scenarios , on page 81 provides the information about troubleshooting your configuration

*Table 12: Troubleshooting Scenarios*

| Problem | Solution |
|---|---|
| **Clock selection** | • Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command.<br>• Ensure that the nonrevertive configurations are in place.<br>• Reproduce the issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm commands. Contact Cisco Technical Support if the issue persists. |

| Problem | Solution |
|---|---|
| **Incorrect QL values** | • Ensure that there is no framing mismatch with the SSM option.<br>• Reproduce the issue using the debug network-clock errors and debug network-clock event commands. |
| **Alarms** | • Reproduce the issue using the debug platform network-clock command enabled in the RSP. Alternatively, enable the debug network-clock event and debug network-clock errors commands. |
| **Incorrect clock limit set or queue limit disabled mode** | • Verify that there are no alarms on the interfaces using the show network-clock synchronization detail command.<br>• Use the **show network-clock synchronization** command to confirm if the system is in revertive mode or nonrevertive mode and verify the non-revertive configurations.<br>• Reproduce the current issue and collect the logs using the debug network-clock errors, debug network-clock event, and debug network-clock sm RSP commands. |
| **Incorrect QL values** when you use the **show network-clock synchronization detail** command. | • Use the **network clock synchronization SSM** (*option 1* \|*option 2*) command to confirm that there is no framing mismatch. Use the **show run interface** command to validate the framing for a specific interface. For the SSM option 1, framing should be SDH or E1, and for SSM option 2, it should be T1.<br>• Reproduce the issue using the debug network-clock errors and debug network-clock event RSP commands. |

**Note** Effective from Cisco IOS XE Everest 16.6.1, on RSP3 module, alarm notification is enabled on 900 watts DC power supply. There are 2 input feeds for 900 watts DC power supply, if one of the input voltage is lesser than the operating voltage, critical alarm is generated for that particular feed and clears (stops) once the voltage is restored but the power supply state remains in OK state as the other power supply is operationally up.

# Configuration Examples

This section contains sample configurations for clocking features on the chassis.

**Note** This section contains partial chassis configurations intended to demonstrate a specific feature.

### Ordinary Clock—Client

```
ptp clock ordinary domain 0
clock-port Client slave
transport ipv4 unicast interface loopback 0 negotiation
clock-source 8.8.8.1
announce timeout 7
delay-req interval 100
```

### Ordinary Clock —Client Mode (Ethernet)

```
ptp clock ordinary domain 0
clock-port Client slave
transport ethernet unicast
clock-source 1234.5678.90ab bridge-domain 2 5
```

### Ordinary Clock—Server

```
ptp clock ordinary domain 0
clock-port Server master
transport ipv4 unicast interface loopback 0 negotiation
```

### Ordinary Clock—Server (Ethernet)

```
ptp clock ordinary domain 0
clock-port Server master
transport ethernet unicast
clock destination interface GigabitEthernet0/0/1
```

### Unicast Configuration—Client Mode

```
ptp clock ordinary domain 0
clock-port Client slave
transport ipv4 unicast interface loopback 0
clock-source 8.8.8.1
```

### Unicast Configuration—Client Mode (Ethernet)

```
ptp clock ordinary domain 0
  clock-port Client slave
    transport ethernet unicast
      clock source 1234.5678.90ab bridge-domain 5 2
```

### Unicast Configuration—Server Mode

```
ptp clock ordinary domain 0
clock-port Server master
transport ipv4 unicast interface loopback 0
clock-destination 8.8.8.2
sync interval 1
announce interval 2
```

### Unicast Configuration—Server Mode (Ethernet)

```
ptp clock ordinary domain 0
  clock-port Server master
    transport ethernet unicast
      clock destination 1234.5678.90ab bridge-domain 5
```

### Unicast Negotiation—Client

```
ptp clock ordinary domain 0
clock-port Client slave
transport ipv4 unicast interface loopback 0 negotiation
clock-source 8.8.8.1
```

### Unicast Negotiation—Client (Ethernet)

```
ptp clock ordinary domain 0
  clock-port Client slave
    transport ethernet unicast negotiation
      clock source 1234.5678.90ab bridge-domain 5 5
  clock-port Client1 slave
    transport ethernet unicast negotiation
      clock source 1234.9876.90ab interface gigabitethernet 0/0/4 2
```

### Unicast Negotiation—Server

```
ptp clock ordinary domain 0
clock-port Server master
transport ipv4 unicast interface loopback 0 negotiation
sync interval 1
announce interval 2
```

### Unicast Negotiation—Server (Ethernet)

```
ptp clock ordinary domain 0
clock-port Server master
transport ethernet unicast negotiation
```

### Boundary Clock

```
ptp clock boundary domain 0
 clock-port Client slave
  transport ipv4 unicast interface Loopback 0 negotiation
  clock source 133.133.133.133
 clock-port Server master
  transport ipv4 unicast interface Loopback 1 negotiation
```

### Transparent Clock

```
ptp clock e2e-transparent domain 0
```

### Hybrid Clock—Boundary

```
ptp clock boundary domain 0 hybrid
```

```
 clock-port Client slave
  transport ipv4 unicast interface Loopback0 negotiation
  clock source 133.133.133.133
 clock-port Server master
  transport ipv4 unicast interface Loopback1 negotiation
Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

### Hybrid Clock—Client

```
ptp clock ordinary domain 0 hybrid
 clock-port Client slave
  transport ipv4 unicast interface Loopback 0 negotiation
  clock source 133.133.133.133

Network-clock input-source 10 interface gigabitEthernet 0/4/0
```

### PTP Redundancy—Client

```
ptp clock ordinary domain 0
 clock-port Client slave
  transport ipv4 unicast interface Loopback 0 negotiation
  clock source 133.133.133.133 1
   clock source 55.55.55.55 2
   clock source 5.5.5.5
```

### PTP Redundancy—Boundary

```
ptp clock boundary domain 0
clock-port Client slave
transport ipv4 unicast interface Loopback 0 negotiation
clock source 133.133.133.133 1
clock source 55.55.55.55 2
clock source 5.5.5.5
clock-port Server master
transport ipv4 unicast interface Lo1 negotiation
```

### Hop-By-Hop PTP Redundancy—Client

```
ptp clock ordinary domain 0
 clock-port Client slave
  transport ipv4 unicast interface Loopback 0 negotiation single-hop
  clock source 133.133.133.133 1
   clock source 55.55.55.55 2
   clock source 5.5.5.5
```

### Hop-By-Hop PTP Redundancy—Boundary

```
ptp clock boundary domain 0
clock-port Client slave
transport ipv4 unicast interface Loopback 0 negotiation single-hop
clock source 133.133.133.133 1
clock source 55.55.55.55 2
clock source 5.5.5.5
```

```
clock-port Server master
transport ipv4 unicast interface Lo1 negotiation single-hop
```

### Time of Day Source—Server

```
TOD-clock 10 gps R0/R1
```

### Time of Day Source—Client

```
TOD-clock 10 ptp domain 0
```

### Clock Selection Parameters

```
network-clock synchronization automatic
network-clock synchronization mode QL-enabled
network-clock input-source 1 ptp domain 3
```

### ToD/1PPS Configuration—Server

```
network-clock input-source 1 external R010m
ptp clock ordinary domain 1
tod R0 ntp
input 1pps R0
clock-port Server master
transport ipv4 unicast interface loopback 0
```

### ToD/1PPS Configuration—Client

```
ptp clock ordinary domain 1
tod R0 ntp
output 1pps R0 offset 200 pulse-width 20 µsec
clock-port Client slave
transport ipv4 unicast interface loopback 0 negotiation
clock source 33.1.1.
```

### Show Commands

```
Router# show ptp clock dataset ?
  current          currentDS dataset
  default          defaultDS dataset
  parent           parentDS dataset
  time-properties  timePropertiesDS dataset
Router# show ptp port dataset ?
 foreign-master  foreignMasterDS dataset
 port            portDS dataset
Router# show ptp clock running domain 0
                      PTP Ordinary Clock [Domain 0]
         State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
         ACQUIRING      1              98405          296399         Track one
                               PORT SUMMARY
   PTP Master
Name                 Tx Mode      Role          Transport    State         Sessions     Port
Addr
Client        unicast      slave              Lo0          Slave               1
8.8.8.8
                             SESSION INFORMATION
```

```
SLAVE [Lo0] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs
 8.8.8.8            296399     98405      0          0
Router#
Router# show platform software ptpd stat stream 0
LOCK STATUS : PHASE LOCKED
SYNC Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 0, Acting Interval 0
  Tx packets : 0,  Rx Packets : 169681
  Last Seq Number : 0,  Error Packets : 1272
Delay Req Packet Stats
  Time elapsed since last packet: 0.0
  Configured Interval : 0, Acting Interval : 0
  Tx packets : 84595, Rx Packets : 0
  Last Seq Number : 19059, Error Packets : 0
!output omitted for brevity
Current Data Set
  Offset from master :  0.4230440
  Mean Path Delay :  0.0
  Steps Removed 1
General Stats about this stream
  Packet rate : 0, Packet Delta (ns) : 0
  Clock Stream handle : 0, Index : 0
  Oper State : 6, Sub oper State : 7
  Log mean sync Interval : -5, log mean delay req int : -4
Router# show platform ptp all
Slave info  : [Loopback0][0x38A4766C]
--------------------------------
clock role          : SLAVE
Slave Port hdl      : 486539266
Tx Mode             : Unicast-Negotiation
Slave IP            : 4.4.4.4
Max Clk Srcs        : 1
Boundary Clock      : FALSE
Lock status         : HOLDOVER
Refcnt              : 1
Configured-Flags    : 0x7F - Clock Port Stream
Config-Ready-Flags  : Port Stream
----------
PTP Engine Handle   : 0
Master IP           : 8.8.8.8
Local Priority      : 0
Set Master IP       : 8.8.8.8
Router#show platform ptp tod all
--------------------------------
ToD/1PPS Info for 0/0
--------------------------------
ToD CONFIGURED        : YES
ToD FORMAT            : NMEA
ToD DELAY             : 0
1PPS MODE             : OUTPUT
OFFSET                : 0
PULSE WIDTH           : 0
ToD CLOCK             : Mon Jan 1  00:00:00 UTC 1900
Router# show ptp clock running domain 0
                      PTP Boundary Clock [Domain 0]
State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
PHASE_ALIGNED  2              32355          159516         Hot standby
PORT SUMMARY

  PTP Master
Name               Tx Mode      Role         Transport State        Sessions Port Addr
```

```
SLAVE              unicast      slave        Ethernet                            1
  9.9.9.1
MASTER             unicast      master       Ethernet  -                 2            -
                             SESSION INFORMATION

SLAVE [Ethernet] [Sessions 1]
 Peer addr          Pkts in    Pkts out   In Errs    Out Errs

 9.9.9.1            159083     31054      0          0

MASTER [Ethernet] [Sessions 2]
 Peer addr                             Pkts in    Pkts out   In Errs    Out Errs
 aabb.ccdd.ee01 [Gig0/2/3]                 223        667        0          0
 aabb.ccdd.ee02 [BD 1000]                    210        634        0          0
```

### Input Synchronous Ethernet Clocking

The following example shows how to configure the chassis to use the BITS interface and two Gigabit Ethernet interfaces as input synchronous Ethernet timing sources. The configuration enables SSM on the BITS port.

```
!
Interface GigabitEthernet0/0
    synchronous mode
    network-clock wait-to-restore 720
!
Interface GigabitEthernet0/1
    synchronous mode
!
!
network-clock synchronization automatic
network-clock input-source 1 External R0 e1 crc4
network-clock input-source 1 gigabitethernet 0/0
network-clock input-source 2 gigabitethernet 0/1
network-clock synchronization mode QL-enabled
no network-clock revertive
```

CHAPTER 5

# Using the Management Ethernet Interface

This chapter covers the following topics:



## Gigabit Ethernet Management Interface Overview

The chassis has one Gigabit Ethernet Management Ethernet interface on each Route Switch Processor.

The purpose of this interface is to allow users to perform management tasks on the router; it is basically an interface that should not and often cannot forward network traffic but can otherwise access the router, often via Telnet and SSH, and perform most management tasks on the router. The interface is most useful before a router has begun routing, or in troubleshooting scenarios when the interfaces are inactive.

The following aspects of the Management Ethernet interface should be noted:

- Each RSP has a Management Ethernet interface, but only the active RSP has an accessible Management Ethernet interface (the standby RSP can be accessed using the console port, however).
- IPv4, IPv6, and ARP are the only routed protocols supported for the interface.
- The interface provides a method of access to the router even if the interfaces or the IOS processes are down.
- The Management Ethernet interface is part of its own VRF. For more information, see the Gigabit Ethernet Management Interface VRF, on page 90.

## Gigabit Ethernet Port Numbering

The Gigabit Ethernet Management port is always GigabitEthernet0.

In a dual RSP configuration, the Management Ethernet interface on the active RSP will always be Gigabit Ethernet 0, while the Management Ethernet interface on the standby RSP will not be accessible using the Cisco IOS CLI in the same telnet session. The standby RSP can be accessed via console port using telnet.

The port can be accessed in configuration mode like any other port on the chassis.

```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitethernet0
Router(config-if)#
```

# IP Address Handling in ROMmon and the Management Ethernet Port

IP addresses can be configured using ROMmon (**IP_ADDRESS=** and **IP_SUBNET_MASK=** commands) and the IOS command-line interface (the **ip address** command in interface configuration mode).

Assuming the IOS process has not begun running on the chassis, the IP address that was set in ROMmon acts as the IP address of the Management Ethernet interface. In cases where the IOS process is running and has taken control of the Management Ethernet interface, the IP address specified when configuring the Gigabit Ethernet 0 interface in the IOS CLI becomes the IP address of the Management Ethernet interface. The ROMmon-defined IP address is only used as the interface address when the IOS process is inactive.

For this reason, the IP addresses specified in ROMmon and in the IOS CLI can be identical and the Management Ethernet interface will function properly in single RSP configurations.

In dual RSP configurations, however, users should never configure the IP address in the ROMmon on either RP0 or RP1 to match each other or the IP address as defined by the IOS CLI. Configuring matching IP addresses introduces the possibility for an active and standby Management Ethernet interface having the same IP address with different MAC addresses, which will lead to unpredictable traffic treatment or possibility of an RSP boot failure.

# Gigabit Ethernet Management Interface VRF

The Gigabit Ethernet Management interface is automatically part of its own VRF. This VRF, which is named “Mgmt-intf,” is automatically configured on the chassis and is dedicated to the Management Ethernet interface; no other interfaces can join this VRF. Therefore, this VRF does not participate in the MPLS VPN VRF or any other network-wide VRF.

Placing the management ethernet interface in its own VRF has the following effects on the Management Ethernet interface:

- Many features must be configured or used inside the VRF, so the CLI may be different for certain Management Ethernet functions on the chassis than on Management Ethernet interfaces on other routers.
- Prevents transit traffic from traversing the router. Because all of the interfaces and the Management Ethernet interface are automatically in different VRFs, no transit traffic can enter the Management Ethernet interface and leave an interface, or vice versa.
- Improved security of the interface. Because the Mgmt-intf VRF has its own routing table as a result of being in its own VRF, routes can only be added to the routing table of the Management Ethernet interface if explicitly entered by a user.

The Management Ethernet interface VRF supports both IPv4 and IPv6 address families.

# Common Ethernet Management Tasks

Because users can perform most tasks on a router through the Management Ethernet interface, many tasks can be done by accessing the router through the Management Ethernet interface.

This section documents common configurations on the Management Ethernet interface and includes the following sections:

## Viewing the VRF Configuration

The VRF configuration for the Management Ethernet interface is viewable using the **show running-config vrf** command.

This example shows the default VRF configuration:

```
Router# show running-config vrf
Building configuration...
Current configuration : 351 bytes
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
(some output removed for brevity)
```

## Viewing Detailed VRF Information for the Management Ethernet VRF

To see detailed information about the Management Ethernet VRF, enter the **show vrf detail Mgmt-intf** command.

```
Router# show vrf detail Mgmt-intf
VRF Mgmt-intf (VRF Id = 4085); default RD <not set>; default VPNID <not set>
  Interfaces:
    Gi0
Address family ipv4 (Table ID = 4085 (0xFF5)):
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 (Table ID = 503316481 (0x1E000001)):
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

# Setting a Default Route in the Management Ethernet Interface VRF

To set a default route in the Management Ethernet Interface VRF, enter the following command

**ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0** *next-hop-IP-address*

# Setting the Management Ethernet IP Address

The IP address of the Management Ethernet port is set like the IP address on any other interface.

Below are two simple examples of configuring an IPv4 address and an IPv6 address on the Management Ethernet interface.

### IPv4 Example

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ip address A.B.C.D A.B.C.D
```

### IPv6 Example

```
Router(config)# interface GigabitEthernet 0
```

Router(config-if)# **ipv6 address** *X:X:X:X::X*

# Telnetting over the Management Ethernet Interface

Telnetting can be done through the VRF using the Management Ethernet interface.

In the following example, the router telnets to 172.17.1.1 through the Management Ethernet interface VRF:

```
Router# telnet 172.17.1.1 /vrf Mgmt-intf
```

# Pinging over the Management Ethernet Interface

Pinging other interfaces using the Management Ethernet interface is done through the VRF.

In the following example, the router pings the interface with the IP address of 172.17.1.1 through the Management Ethernet interface.

```
Router# ping vrf Mgmt-intf 172.17.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

# Copy Using TFTP or FTP

To copy a file using TFTP through the Management Ethernet interface, the **ip tftp source-interface GigabitEthernet 0** command must be entered before entering the **copy tftp** command because the **copy tftp** command has no option of specifying a VRF name.

Similarly, to copy a file using FTP through the Management Ethernet interface, the **ip ftp source-interface GigabitEthernet 0** command must be entered before entering the **copy ftp** command because the **copy ftp** command has no option of specifying a VRF name.

### TFTP Example

```
Router(config)# ip tftp source-interface gigabitethernet 0
```

### FTP Example

```
Router(config)# ip ftp source-interface gigabitethernet 0
```

# NTP Server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server over the Management Ethernet interface, enter the **ntp server vrf Mgmt-intf** command and specify the IP address of the device providing the update.

The following CLI provides an example of this procedure.

```
Router(config)# ntp server vrf Mgmt-intf 172.17.1.1
```

# SYSLOG Server

To specify the Management Ethernet interface as the source IPv4 or IPv6 address for logging purposes, enter the **logging host** *ip-address* **vrf Mgmt-intf** command.

The following CLI provides an example of this procedure.

```
Router(config)# logging host <ip-address> vrf Mgmt-intf
```

# SNMP-related services

To specify the Management Ethernet interface as the source of all SNMP trap messages, enter the **snmp-server source-interface traps gigabitEthernet 0** command.

The following CLI provides an example of this procedure:

```
Router(config)# snmp-server source-interface traps gigabitEthernet 0
```

# Domain Name Assignment

The IP domain name assignment for the Management Ethernet interface is done through the VRF.

To define the default domain name as the Management Ethernet VRF interface, enter the **ip domain-name vrf Mgmt-intf** *domain* command.

```
Router(config)# ip domain-name vrf Mgmt-intf cisco.com
```

# DNS service

To specify the Management Ethernet interface VRF as a name server, enter the **ip name-server vrf Mgmt-intf** *IPv4-or-IPv6-address* command.

```
Router(config)# ip name-server vrf Mgmt-intf
 IPv4-or-IPv6-address
```

# RADIUS or TACACS+ Server

To group the Management VRF as part of a AAA server group, enter the **ip vrf forward Mgmt-intf** command when configuring the AAA server group.

The same concept is true for configuring a TACACS+ server group. To group the Management VRF as part of a TACACS+ server group, enter the **ip vrf forwarding Mgmt-intf** command when configuring the TACACS+ server group.

### Radius Server Group Configuration

```
Router(config)# aaa group server radius hello
Router(config-sg-radius)# ip vrf forwarding Mgmt-intf
```

### Tacacs+ Server Group Example

```
outer(config)# aaa group server tacacs+ hello
Router(config-sg-tacacs+)# ip vrf forwarding Mgmt-intf
```

# VTY lines with ACL

To ensure an access control list (ACL) is attached to vty lines that are and are not using VRF, use the **vrf-also** option when attaching the ACL to the vty lines.

```
Router(config)# line vty 0 4
Router(config-line)# access-class 90 in vrf-also
```

CHAPTER 6

# Configuring Ethernet Interfaces

This chapter provides information about configuring the Gigabit Ethernet interface modules.

For more information about the commands used in this chapter, see the Cisco IOS XE 3S Command References.



# Configuring Ethernet Interfaces

This section describes how to configure the Gigabit and Ten Gigabit Ethernet interface modules and includes information about verifying the configuration.

## Limitations and Restrictions

- Interface module A900-IMA8Z in slot 0 with A900-RSP3C-200-S supports a maximum of 6 ports at 10GE speed and needs explicit enablement using the **hw-module subslot 0/0 A900-IMA8Z mode 6-port** command.
- VRF-Aware Software Infrastructure (VASI) interface commnads **interface vasileft** and interface vasiright are not supported .
- Interface modules have slot restrictions, see NCS 4200 Hardware Installation Guides.
- MPLS MTU is *not* supported.
- On the RSP3 module, MTU value configured for a BDI interface should match with the MTU configuration for all the physical interfaces, which have a service instance associated with this BDI.
- If the packet size is more than the configured MTU value and exceeds 1Mbps, packets are dropped. Packets are fragmented when the packet size is more than the configured MTU value and when traffic is lesser than 1Mbps.
- To replace the configured interface module with a different interface module in a particular slot, run the **hw-module subslot *slot-num* default** command.
- Giant counters are not supported.

- Ingress counters are not incremented for packets of the below packet format on the RSP3 module for the 10 Gigabit Ethernet interfaces, 100 Gigabit Ethernet interfaces, and 40 Gigabit Ethernet interfaces:

  MAC header---->Vlan header---->Length/Type

  When these packets are received on the RSP3 module, the packets are not dropped, but the counters are not incremented.

- If the IM is shutdown using **hw-module subslot shutdown** command, then the IM goes out-of-service. You should perform a Stateful Switchover (SSO) in the interim, as the IM needs to be re-inserted for successful reactivation.

- Following are some of the IMs that are not supported on certain slots when IPsec license is enabled:

  - The below IMs are not supported on the Slot 11 on the Cisco ASR 907 router:

    - SPA_TYPE_ETHER_IM_8x10GE
    - SPA_TYPE_ETHER_IM_2x40GE

  - The below IMs are not supported on the Slot 2 on the Cisco ASR 903 router for RSP3-200 and RSP3-400:

    - SPA_TYPE_ETHER_IM_8xGE_SFP_1x10GE
    - SPA_TYPE_ETHER_IM_8xGE_CU_1x10GE
    - SPA_TYPE_ETHER_IM_1x10GE
    - SPA_TYPE_ETHER_IM_8x10GE
    - SPA_TYPE_OCX_IM_OC3OC12
    - SPA_TYPE_ETHER_IM_8xGE_SFP
    - SPA_TYPE_ETHER_IM_8xGE_CU

- CTS signal goes down, when control signal frequency is configured more than 5000 ms and timeout setting is more than 20,000 ms (4x control_frequency), which is greater than the OIR time (~20s) for a selected subordinate to complete an OIR cycle. This results in the primary being unaware that the subordinate is down and CTS of all subordinates are down too. To avoid this situation, ensure that the timeout is shorter than the OIR time of the subordinate. Set the control frequency to less than or equal to 5000 ms and the timeout setting to less than or equal to 20,000 ms before you perform OIR.

- You may ignore the following error that is seen during IM OIR or while the router goes down:

  ```
  %IOSXE-2-PLATFORM: R1/0: kernel: Address caused MCE = 0x0, DEAR = <>
  ```

# Configuring an Interface

This section lists the required configuration steps to configure Gigabit and Ten Gigabit Ethernet interface modules.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | Do one of the following:<br>• **interface gigabitethernet** *slot/subslot/port*<br>• **interface tengigabitethernet** *slot/subslot/port*<br>**Example:**<br>`Router(config)# interface gigabitethernet 0/0/1`<br>**Example:**<br>**Example:**<br>`Router(config)# interface tengigabitethernet 0/0/1` | Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface to configure and enters interface configuration mode, where:<br>**Note** The slot number is always 0. |
| **Step 3** | **ip address** *ip-address mask* {**secondary**} \| **dhcp** {**client-id** *interface-name*} {**hostname** *host-name*}]<br>**Example:**<br>`Router(config-if)# ip address 192.168.1.1 255.255.255.255 dhcp hostname host1` | Sets a primary or secondary IP address for an interface that is using IPv4, where:<br>• *ip-address* —The IP address for the interface.<br>• *mask* —The mask for the associated IP subnet.<br>• **secondary**—(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.<br>• **dhcp**—Specifies that IP addresses will be assigned dynamically using DHCP.<br>• **client-id** *interface-name*—Specifies the client identifier. The *interface-name* sets the client identifier to the hexadecimal MAC address of the named interface.<br>• **hostname** *host-name*—Specifies the hostname for the DHCP purposes. The *host-name* is the name of the host to be placed in the DHCP option 12 field. |
| **Step 4** | **no negotiation auto**<br>**Example:**<br>`Router(config-if)# no negotiation auto` | (Optional) Disables automatic negotitation.<br>**Note** Use the **speed** command only when the mode is set to no negotiation auto. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **speed**{ **10** \| **100** \| **1000**}<br>**Example:**<br>`Router(config-if)# speed 1000` | (Optional) Specifies the speed for an interface to transmit at 10, 100, and 1000 Mbps (1 Gbps), where the default is 1000 Mbps. |
| **Step 6** | **mtu** *bytes*<br>**Example:**<br>`Router(config-if)# mtu 1500` | (As Required) Specifies the maximum packet size for an interface, where:<br>• *bytes*—The maximum number of bytes for a packet.<br>The default is 1500 bytes; the range is from 1500 to 9216. |
| **Step 7** | **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]<br>**Example:**<br>`Router(config-if)# standby 250 ip 192.168.10.1` | Creates or enables the Hot Standby Router Protocol (HSRP) group using its number and virtual IP address, where:<br>• (Optional) *group-number*—The group number on the interface for which HSRP is being enabled. The range is from 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number.<br>• ( Optional on all but one interface if configuring HSRP ) *ip-address*—The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces; it can be learned on the other interfaces.<br>• (Optional) **secondary**—Specifies that the IP address is a secondary hot standby router interface. If neither router is designated as a secondary or standby router and no priorities are set, the primary IP addresses are compared and the higher IP address is the active router, with the next highest as the standby router.<br>**Note** This command is required only for configurations that use HSRP.<br>**Note** This command enables HSRP but does not configure it further. |
| **Step 8** | **no shutdown**<br>**Example:**<br>`Router(config-if)# no shutdown` | Enables the interface. |

# Specifying the Interface Address on an Interface Module

To configure or monitor Ethernet interfaces, you need to specify the physical location of the interface module and interface in the CLI. The interface address format is slot/subslot/port, where:

- slot—The chassis slot number in the chassis where the interface module is installed.

**Note** The interface module slot number is always 0.

- subslot—The subslot where the interface module is installed. Interface module subslots are numbered from 0 to 5 for ASR 903 and from 0 to 15 for ASR 907, from bottom to top.
- port—The number of the individual interface port on an interface module.

The following example shows how to specify the first interface (0) on an interface module installed in the first interface module slot:

```
Router(config)# interface GigabitEthernet 0/0/0
 no ip address
 shutdown
 negotiation auto
 no cdp enable
```

# Configuring Hot Standby Router Protocol

Hot Standby Router Protocol (HSRP) provides high network availability because it routes IP traffic from hosts without relying on the availability of any single router. You can deploy HSRP in a group of routers to select an active router and a standby router. (An *active* router is the router of choice for routing packets; a *standby* router is a router that takes over the routing duties when an active router fails, or when preset conditions are met).

HSRP is enabled on an interface by entering the **standby** [*group-number*] **ip** [*ip-address* [**secondary**]] command. The **standby** command is also used to configure various HSRP elements. This document does not discuss more complex HSRP configurations. For additional information on configuring HSRP, see to the HSRP section of the Cisco IP Configuration Guide publication that corresponds to your Cisco IOS XE software release. In the following HSRP configuration, standby group 2 on Gigabit Ethernet port 0/1/0 is configured at a priority of 110 and is also configured to have a preemptive delay should a switchover to this port occur:

```
Router(config)#interface GigabitEthernet 0/1/0
Router(config-if)#standby 2 ip 192.168.1.200
Router(config-if)#standby 2 priority 110
Router(config-if)#standby 2 preempt
```

The maximum number of different HSRP groups that can be created on one physical interface is 4. If additional groups are required, create 4 groups on the physical interface, and the remaining groups on the BDI or on another physical interface.

**Note** TCAM space utilization changes when HSRP groups are configured on the router. If HSRP groups are configured the TCAM space is utilized. Each HSRP group takes 1 TCAM entry. The "Out of TCAM" message may be displayed if total number of TCAM space used by HSRP groups and prefixes on the router exceeds scale limit.

> **Note** HSRP state flaps with sub-second "Hello" or "Dead" timers.

#### Restrictions

HSRPv2 is not supported.

## Verifying HSRP

To verify the HSRP information, use the show standby command in EXEC mode:

```
Router# show standby
Ethernet0 - Group 0
Local state is Active, priority 100, may preempt
Hellotime 3 holdtime 10
Next hello sent in 0:00:00
Hot standby IP address is 198.92.72.29 configured
Active router is local
Standby router is 198.92.72.21 expires in 0:00:07
Standby virtual mac address is 0000.0c07.ac00
Tracking interface states for 2 interfaces, 2 up:
UpSerial0
UpSerial1
```

# Modifying the Interface MTU Size

> **Note** The maximum number of unique MTU values that can be configured on the physical interfaces on the chassis is 8. Use the **show platform hardware pp active interface mtu command** to check the number of values currently configured on the router. This is not applicable on Cisco ASR 900 RSP3 Module.

The Cisco IOS software supports three different types of configurable maximum transmission unit (MTU) options at different levels of the protocol stack:

- Interface MTU—The interface module checks the MTU value of incoming traffic. Different interface types support different interface MTU sizes and defaults. The interface MTU defines the maximum packet size allowable (in bytes) for an interface before drops occur. If the frame is smaller than the interface MTU size, but is not smaller than the minimum frame size for the interface type (such as 64 bytes for Ethernet), then the frame continues to process.
- MPLS MTU—If the MPLS MTU is set to a value, for example, 1500 bytes, the value is programmed as 1504 bytes at the hardware level to allow the addition of one label. Consider the case of pseudowire. If the packet size of Layer 2 traffic sent with four bytes of Frame Check Sequence (FCS) to the pseudowire is 1500 bytes, then and four bytes of pseudowire control word and one pseudowire label (label size is four bytes) is added to the packet, the packet size is now 1508 bytes with FCS. However, note that while calculating the packet size, FCS is not considered. So the calculated packet size is 1504 bytes, which is equal to the MPLS MTU programmed in the hardware. This packet is forwarded as expected.

  However, if another label is added to this packet, the packet size becomes 1508 bytes without FCS. This value is greater than programmed MTU value, so this packet is dropped. This restriction applies not only to pseudowire, but to the entire MPLS network.

To ensure that packets are not dropped, MPLS MTUs should be set considering the maximum size of the label stack that is added to the packet in the network.

For the Gigabit Ethernet interface module on the chassis, the default MTU size is 1500 bytes. The maximum configurable MTU is 9216 bytes. The interface module automatically adds an additional 22 bytes to the configured MTU size to accommodate some of the additional overhead.

### Limitations

In EtherLike-MIB, the **dot3StatsFrameTooLongs** frames count in SNMP increases when the frame packet size is more than the default MTU.

## Interface MTU Configuration Guidelines

When configuring the interface MTU size, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following additional overhead:
  - Layer 2 header—14 bytes
  - Dot1q header—4 bytes
  - CRC—4 bytes
- Interface MTU is not supported on BDI Interface

## Configuring Interface MTU

To modify the MTU size on an interface, use the following command in interface configuration mode:

| Command | Purpose |
|---|---|
| **mtu** *bytes*<br><br>`Router(config-if)# mtu bytes` | Configures the maximum packet size for an interface, where:<br>• *bytes*— Specifies the maximum number of bytes for a packet.<br><br>The default is 1500 bytes and the maximum configurable MTU is 9216 bytes. |

To return to the default MTU size, use the **no** form of the command.

**Note** When IP FRR over BDI is configured, the maximum allowed packet size is 1504 bytes.

When the BGP-PIC core is enabled, a packet destined to a prefix that is learnt through eBGP, is dropped if the packet size is greater than 1504 bytes. To work around this limitation, do one of the following:

- Disable the BGP-PIC core,
- Use the static route, or
- Use routed-port instead of BDI.

## Verifying the MTU Size

To verify the MTU size for an interface, use the **show interfaces gigabitethernet** privileged EXEC command and observe the value shown in the "MTU" field.

The following example shows an MTU size of 1500 bytes for interface port 0 (the second port) on the Gigabit Ethernet interface module installed in slot 1:

```
Router# show interfaces gigabitethernet 0/1/0
GigabitEthernet0/1/0 is up, line protocol is up
  Hardware is  NCS4200-1T8LR-PS, address is d0c2.8216.0590 (bia d0c2.8216.0590)
  MTU 1500 bytes
, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 22/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

# Configuring the Encapsulation Type

The only encapsulation supported by the interface modules is IEEE 802.1Q encapsulation for virtual LANs (VLANs).

**Note** VLANs are only supported on Ethernet Virtual Connection (EVC) service instances and Trunk Ethernet Flow Point (EFP) interfaces.

# Configuring Autonegotiation on an Interface

Gigabit Ethernet interfaces use a connection-setup algorithm called *autonegotiation.* Autonegotiation allows the local and remote devices to configure compatible settings for communication over the link. Using autonegotiation, each device advertises its transmission capabilities and then agrees upon the settings to be used for the link.

For the Gigabit Ethernet interfaces on the chassis, flow control is autonegotiated when autonegotiation is enabled. Autonegotiation is enabled by default.

When enabling autonegotiation, consider these guidelines:

- If autonegotiation is disabled on one end of a link, it must be disabled on the other end of the link. If one end of a link has autonegotiation disabled while the other end of the link does not, the link will not come up properly on both ends.
- Flow control is enabled by default.
- Flow control will be on if autonegotiation is disabled on both ends of the link.

## Enabling Autonegotiation

To enable autonegotiation on a Gigabit Ethernet interface, use the following command in interface configuration mode:

| Command | Purpose |
| --- | --- |
| **negotiation auto**<br><br>`Router(config-if)# negotiation auto` | Enables autonegotiation on a Gigabit Ethernet interface. Advertisement of flow control occurs. |

## Disabling Autonegotiation

Autonegotiation is automatically enabled and can be disabled on Gigabit Ethernet interfaces . During autonegotiation, advertisement for flow control, speed, and duplex occurs, depending on the media (fiber or copper) in use.

Speed and duplex configurations can be advertised using autonegotiation. The values that are negotiated are:

- For Gigabit Ethernet interfaces using RJ-45 ports and for Copper (Cu) SFP ports—10, 100, and 1000 Mbps for speed and full-duplex mode. Link speed is not negotiated when using fiber interfaces.

To disable autonegotiation, use the following command in interface configuration mode:

| Command | Purpose |
| --- | --- |
| **no negotiation auto**<br><br>`Router(config-if)# no negotiation auto` | Disables autonegotiation on Gigabit Ethernet interfaces. No advertisement of flow control occurs. |

# Configuring Carrier Ethernet Features

For information about configuring an Ethernet interface as a layer 2 Ethernet virtual circuit (EVC) or Ethernet flow point (EFP), see the Ethernet Virtual Connections.

# Saving the Configuration

To save your running configuration to NVRAM, use the following command in privileged EXEC configuration mode:

| Command | Purpose |
| --- | --- |
| **copy running-config startup-config**<br><br>`Router# copy running-config startup-config` | Writes the new configuration to NVRAM. |

For information about managing your system image and configuration files, refer to the Cisco IOS Configuration Fundamentals Configuration Guide and Cisco IOS Configuration Fundamentals Command Reference publications that correspond to your Cisco IOS software release.

## Shutting Down and Restarting an Interface

You can shut down and restart any of the interface ports on an interface module independently of each other. Shutting down an interface stops traffic and enters the interface into an "administratively down" state.

If you are preparing for an OIR of an interface module, it is not necessary to independently shut down each of the interfaces prior to deactivation of the module.

| Command | Purpose |
|---|---|
| **shutdown**<br><br>`router#configure terminal`<br>`Enter configuration commands, one per line. End with CNTL/Z.`<br>`router(config)`<br>`router(config)#interface GigabitEthernet 0/1/0`<br>`router(config-if)#shutdown`<br><br>**no shutdown**<br><br>`router#configure terminal`<br>`Enter configuration commands, one per line. End with CNTL/Z.`<br>`router(config)`<br>`router(config)#interface GigabitEthernet 0/1/0`<br>`router(config-if)#no shutdown` | Restarts, stops, or starts an interface. |

# Verifying the Interface Configuration

Besides using the **show running-configuration** command to display the configuration settings, you can use the **show interfaces gigabitethernet** command to get detailed information on a per-port basis for your Gigabit Ethernet interface module.

## Verifying Per-Port Interface Status

To find detailed interface information on a per-port basis for the Gigabit Ethernet interface module, use the **show interfaces gigabitethernet** command.

The following example provides sample output for interface port 0 on the interface module located in slot 1:

```
Router# show interfaces GigabitEthernet0/1/0
GigabitEthernet0/1/0 is up, line protocol is up
  Hardware is  NCS4200-1T8LR-PS, address is d0c2.8216.0590 (bia d0c2.8216.0590)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 08:59:45, output hang never
  Last clearing of show interface counters 09:00:18
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     11 packets input, 704 bytes, 0 no buffer
     Received 11 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

# Verifying Interface Module Status

You can use various **show** commands to view information specific to SFP, XFP, CWDM, and DWDM optical transceiver modules.

**Note** The **show interface transceiver** command is *not* supported on the router.

To check or verify the status of an SFP Module or XFP Module, use the following **show** commands:

Use **show hw-module** *slot/subslot* **transceiver** *port* **status** or **show interfaces** *interface* **transceiver detail** to view the threshold values for temperature, voltage and so on.

For example, **show hw-module subslot 0/5 transceiver 1 status** or **show interfaces tenGigabitEthernet 0/5/1 transceiver detail** .

| Command | Purpose |
|---|---|
| **show hw-module** *slot/subslot* **transceiver** *port* **idprom** | Displays information for the transceiver identification programmable read only memory (idprom).<br>**Note** Transceiver types must match for a connection between two interfaces to become active. |
| **show hw-module** *slot/subslot* **transceiver** *port* **idprom status** | Displays information for the transceiver initialization status.<br>**Note** The transmit and receive optical power displayed by this command is useful for troubleshooting Digital Optical Monitoring (DOM). For interfaces to become active, optical power must be within required thresholds. |
| **show hw-module** *slot/subslot* **transceiver** *port* **idprom dump** | Displays a dump of all EEPROM content stored in the transceiver. |

The following **show hw-module subslot** command sample output is for 1000BASE BX10-U:

```
Router#show hw-module subslot 0/2 transceiver 0 idprom brief

IDPROM for transceiver GigabitEthernet0/2/0:
  Description                               = SFP or SFP+ optics (type 3)
```

```
  Transceiver Type:                         = 1000BASE BX10-U (259)
  Product Identifier (PID)                  = GLC-BX-U
  Vendor Revision                           = 1.0
  Serial Number (SN)                        = NPH20441771
  Vendor Name                               = CISCO-NEO
  Vendor OUI (IEEE company ID)              = 00.15.06 (5382)
  CLEI code                                 = IPUIAG5RAC
  Cisco part number                         = 10-2094-03
 Device State                              = Enabled.
  Date code (yy/mm/dd)                      = 16/11/12
  Connector type                            = LC.
  Encoding                                  = 8B10B (1)
  Nominal bitrate                           = GE (1300 Mbits/s)
  Minimum bit rate as % of nominal bit rate = not specified
  Maximum bit rate as % of nominal bit rate = not specified
Router#
```

The following **show hw-module subslot** command sample output is for an SFP+ 10GBASE-SR:

```
Router#show hw-module subslot 0/2 transceiver 8 idprom brief

IDPROM for transceiver TenGigabitEthernet0/2/8:
  Description                               = SFP or SFP+ optics (type 3)
  Transceiver Type:                         = SFP+ 10GBASE-SR (273)
  Product Identifier (PID)                  = SFP-10G-SR
  Vendor Revision                           = 2
  Serial Number (SN)                        = JUR2052G19W
  Vendor Name                               = CISCO-LUMENTUM
  Vendor OUI (IEEE company ID)              = 00.01.9C (412)
  CLEI code                                 = COUIA8NCAA
  Cisco part number                         = 10-2415-03
  Device State                              = Enabled.
  Date code (yy/mm/dd)                      = 16/12/21
  Connector type                            = LC.
  Encoding                                  = 64B/66B (6)
  Nominal bitrate                           =  (10300 Mbits/s)
  Minimum bit rate as % of nominal bit rate = not specified
  Maximum bit rate as % of nominal bit rate = not specified
Router#
```

**Note** VID for optics displayed in **show inventory** command and vendor revision shown in **idprom detail** command output are stored in diffrent places in Idprom.

# Configuring LAN/WAN-PHY Controllers

The LAN/WAN-PHY controllers are configured in the physical layer control element of the Cisco IOS XE software.

## Restrictions for LAN/WAN-PHY Mode

- Effective with Cisco IOS XE Release 3.18.1SP, A900-IMA8Z Interface Modules (IM) support LAN/WAN-PHY mode.
- The following A900-IMA8Z IM alarms are not supported:

- NEWPTR
- PSE
- NSE
- FELCDP
- FEAISP

# Configuring LAN-PHY Mode

This section describes how to configure LAN-PHY mode on the Gigabit Ethernet interface modules.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show controllers wanphy** *slot/subslot/port*<br>**Example:**<br>`Router# show controllers wanphy 0/1/0`<br><br>`TenGigabitEthernet0/1/0`<br>**`Mode of Operation: WAN Mode`**<br>`SECTION`<br>`LOF = 0              LOS    = 0`<br>`                    BIP(B1) = 0`<br>`LINE`<br>`AIS = 0              RDI    = 0`<br>` FEBE = 0           BIP(B2) = 0`<br>`PATH`<br>`AIS = 0              RDI    = 0`<br>` FEBE = 0           BIP(B3) = 0`<br>`LOP = 0              NEWPTR = 0`<br>` PSE  = 0           NSE     = 0`<br>`WIS ALARMS`<br>`SER    = 0           FELCDP = 0`<br>` FEAISP = 0`<br>`WLOS   = 0           PLCD   = 0`<br>`LFEBIP = 0           PBEC   = 0`<br>`Active Alarms[All defects]: SWLOF LAIS`<br>`PAIS SER`<br>`Active Alarms[Highest Alarms]: SWLOF`<br>`Alarm reporting enabled for: SF SWLOF`<br>`B1-TCA B2-TCA PLOP WLOS`<br>`Rx(K1/K2): 00/00  Tx(K1/K2): 00/00`<br>`S1S0 = 00, C2 = 0x1A`<br>`PATH TRACE BUFFER: UNSTABLE`<br>`Remote J1 Byte :`<br>`BER thresholds:  SD = 10e-6  SF = 10e-3`<br>`TCA thresholds:  B1 = 10e-6  B2 = 10e-6`<br>`  B3 = 10e-6` | Displays the configuration mode of the LAN/WAN-PHY controller. Default configuration mode is LAN.<br><br>If the configuration mode is WAN, complete the rest of the procedure to change the configuration mode to LAN.<br><br>• *slot* /*subslot* /*port*—The location of the interface. |
| **Step 2** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# configure terminal` | |
| **Step 3** | Do the following:<br>• **hw-module subslot** *slot/subslot* **interface** *port* **enable LAN**<br>**Example:**<br>`Router(config)# hw-module subslot 0/1 enable LAN`<br>**Example:**<br>`Router(config)# hw-module subslot 0/1 interface 1 enable LAN` | Configures LAN-PHY mode for the Ethernet interface module.<br>• *slot* /*subslot* /*port*—The location of the interface.<br>Use the **hw-module subslot** *slot/subslot* **interface** *port enable LAN* command to configure the LAN-PHY mode for the Ethernet interface module. |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode and enters privileged EXEC mode. |
| **Step 5** | **show controllers wanphy** *slot/subslot/port*<br>**Example:**<br>`Router# show controllers wanphy 0/1/2`<br>`TenGigabitEthernet0/1/2`<br>**`Mode of Operation: LAN Mode`** | Displays configuration mode for the LAN/WAN-PHY controller. The example shows the mode of operation as LAN mode for the Cisco 8-Port 10 Gigabit Ethernet LAN/WAN-PHY Controller. |

# Configuring WAN-PHY Mode

This section describes how to configure WAN-PHY mode on the Gigabit Ethernet interface modules.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show controllers wanphy** *slot/subslot/port*<br>**Example:**<br>`Router# show controllers wanphy 0/1/0`<br>`TenGigabitEthernet0/1/0`<br>**`Mode of Operation: LAN Mode`** | Displays the configuration mode of the WAN-PHY controller. Default configuration mode is LAN.<br>• *slot* /*subslot* /*port*—The location of the interface. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | Do the following:<br>• **hw-module subslot** *slot/subslot***interface** *port enable WAN*<br>**Example:**<br>`Router(config)# hw-module subslot 0/1 enable WAN`<br>**Example:**<br>`Router(config)# hw-module subslot 0/1 interface 1 enable WAN` | Configures WAN-PHY mode for the Ethernet interface module.<br>• *slot* /*subslot* /*port* —The location of the interface.<br>Use the **hw-module subslot** *slot/subslot* **interface** *port enable WAN* command to configure the WAN-PHY mode for the Ethernet interface module. |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode and enters privileged EXEC mode. |
| **Step 5** | **show controllers wanphy** *slot/subslot/port*<br>**Example:**<br>`Router# show controllers wanphy 0/1/5`<br>`TenGigabitEthernet0/1/5`<br>**`Mode of Operation: WAN Mode`**<br>`SECTION`<br>`  LOF = 0              LOS    = 0`<br>`                     BIP(B1) = 0`<br>`LINE`<br>`  AIS = 0              RDI    = 0`<br>`   FEBE = 0          BIP(B2) = 0`<br>`PATH`<br>`  AIS = 0              RDI    = 0`<br>`   FEBE = 0          BIP(B3) = 0`<br>`  LOP = 0              NEWPTR = 0`<br>`   PSE  = 0          NSE     = 0`<br>`WIS ALARMS`<br>`  SER    = 0           FELCDP = 0`<br>`   FEAISP = 0`<br>`  WLOS   = 0           PLCD   = 0`<br><br>`  LFEBIP = 0           PBEC   = 0`<br><br>`Active Alarms[All defects]: SWLOF LAIS PAIS SER`<br>`Active Alarms[Highest Alarms]: SWLOF`<br>`Alarm reporting enabled for: SF SWLOF B1-TCA B2-TCA PLOP WLOS`<br>`  Rx(K1/K2): 00/00  Tx(K1/K2): 00/00`<br>`  S1S0 = 00, C2 = 0x1A`<br>`PATH TRACE BUFFER: UNSTABLE`<br>`Remote J1 Byte :`<br>`BER thresholds:  SD = 10e-6  SF = 10e-3`<br>`TCA thresholds:  B1 = 10e-6  B2 = 10e-6`<br>`  B3 = 10e-6` | Displays configuration mode for the LAN/WAN-PHY controller. The example shows the mode of operation as WAN mode for the Cisco 8-Port 10 Gigabit Ethernet LAN/WAN-PHY Controller. |

# Configuring WAN-PHY Error Thresholds

This section describes how to configure WAN-PHY Signal Failure (SF) and Signal Degrade (SD) Bit Error Rate (BER) reporting and thresholds.

An SF alarm is triggered if the line bit error (B2) rate exceeds a user-provisioned threshold range (over the range of 10e-3 to 10e-9).

An SD alarm is declared if the line bit error (B2) rate exceeds a user-provisioned threshold range (over the range of 10e-3 to 10e-9). If the B2 errors cross the SD threshold, a warning about link quality degradation is triggered. The WAN-PHY alarms are useful for some users who are upgrading their Layer 2 core network from a SONET ring to a 10-Gigabit Ethernet ring.

### Before you begin

The controller must be in the WAN-PHY mode before configuring the SF and SD BER reporting and thresholds.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **controller wanphy** *slot/subslot/port*<br>**Example:**<br>`Router(config)# controller wanphy 0/3/0` | Enters WAN physical controller configuration mode in which you can configure a 10-Gigabit Ethernet WAN-PHY controller.<br>*slot* /*subslot* /*port* —The location of the interface. |
| **Step 3** | **wanphy** {**delay** \| **flag** \| **report-alarm** \| **threshold** {**b1-tca** \| **b2-tca** \| **sd-ber** \| **sf-ber** [*bit error rate*]}}<br>**Example:**<br>`Router(config-controller)# wanphy threshold b1-tca 6` | Configures WAN-PHY controller processing.<br>• delay—Delays WAN-PHY alarm triggers.<br>• flag—Specifies byte values.<br>• report-alarm—Configures WAN-PHY alarm reporting.<br>• threshold—Sets BER threshold values.<br>  • b1-tca—Sets B1 alarm BER threshold.<br>  • b2-tca—Sets B2 alarm BER threshold.<br>  • sd-ber—Sets Signal Degrade BER threshold.<br>  • sf-ber—Sets Signal Fail BER threshold.<br>• bit error rate— Specifies bit error rate. |
| **Step 4** | **end**<br>**Example:** | Exits controller configuration mode and enters privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | Router(config-controller)# end | |

# Configuration Examples

## Example: Basic Interface Configuration

The following example shows how to enter the global configuration mode to configure an interface, configure an IP address for the interface, and save the configuration:

```
! Enter global configuration mode.

!

Router# configure terminal

! Enter configuration commands, one per line. End with CNTL/Z.

!

! Specify the interface address.

!

Router(config)# interface gigabitethernet 0/0/1

!

! Configure an IP address.

!

Router(config-if)# ip address 192.168.50.1 255.255.255.0

!

! Start the interface.

!

Router(config-if)# no shut

!
```

```
! Save the configuration to NVRAM.
!
Router(config-if)# exit
Router# copy running-config startup-config
```

# Example: MTU Configuration

**Note** The maximum number of unique MTU values that can be configured on the physical interfaces on the chassis is eight. Use the **show platform hardware pp active interface mtu command** to check the number of values currently configured on the router.

The following example shows how to set the MTU interface to 9216 bytes.

**Note** The interface module automatically adds an additional 38 bytes to the configured MTU interface size.

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Specify the interface address
!
Router(config)# interface gigabitethernet 0/0/1
!
! Configure the interface MTU.
!
Router(config-if)# mtu 9216
```

# Example: VLAN Encapsulation

The following example shows how to configure interface module port 2 (the third port) and configure the first interface on the VLAN with the ID number 268 using IEEE 802.1Q encapsulation:

```
! Enter global configuration mode.
!
Router# configure terminal
! Enter configuration commands, one per line. End with CNTL/Z.
!
! Enter configuration commands, one per line. End with CNTL/Z.
!
Router(config)# service instance 10 ethernet
!
! Configure dot1q encapsulation and specify the VLAN ID.
Router(config-subif)# encapsulation dot1q 268
!
```

**Note** VLANs are supported only on EVC service instances and Trunk EFP interfaces.

CHAPTER 7

# Configuring T1/E1 Interfaces

This chapter provides information about configuring the T1/E1 interface module on the chassis. It includes the following sections:

For information about managing your system images and configuration files, refer to the Cisco IOS Configuration Fundamentals Configuration Guide and Cisco IOS Configuration Fundamentals Command Reference publications.

For more information about the commands used in this chapter, refer to the Cisco IOS Command Reference publication for your Cisco IOS software release.



# Configuration Tasks

This section describes how to configure the T1/E1 interface module for the chassis and includes the following topics:

## Limitations

This section describes the software limitations that apply when configuring the T1/E1 interface module.

- The following interface modules are not supported on the RSP3 module:
  - 16-port T1/E1 interface module
  - 8-portT1/E1 interface module
  - 32-portT1/E1 interface module
- The **configure replace** command is not supported on the T1/E1 interface modules.
- The chassis does *not* support more than 16 IMA groups on each T1/E1 interface module.
- The chassis only supports the following BERT patterns: 2^11, 2^15, 2^20-O153, and 2^20-QRSS.
- L2TPv3 encapsulation is not supported.
- Replacing a configured interface module with a different interface module in the same slot is not supported.

- Mixed configurations of features are not supported on the same port.
- The Payload calculation per unit for T1/E1 interface module is:
    - Framed E1 / T1 with no. of time Slots less than 4 –> Payload = 4 x no. of time slots.
    - Framed E1 / T1 with no. of Time Slots greater than or equal 4 -> Payload = 2 x no. of time slots.
    - Unframed T1, C11 –> Payload = 48 (2 x 24 (all slots)).
    - Unframed E1, C12 –> Payload = 64 (2 x32(all slots))
- Channelization is not supported for serial interfaces. However, channelization is supported for CEM at the DS0 level.

# Required Configuration Tasks

This section lists the required configuration steps to configure the T1/E1 interface module. Some of the required configuration commands implement default values that might be appropriate for your network. If the default value is correct for your network, then you do not need to configure the command.

## Setting the Card Type

The interface module is not functional until the card type is set. Information about the interface module is not indicated in the output of any show commands until the card type has been set. There is no default card type.

**Note** Mixing of T1 and E1 interface types is not supported. All ports on the interface module must be of the same type.

To set the card type for the T1/E1 interface module, complete these steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **card type** {**e1** \| **t1**} *slot/subslot*<br>**Example:**<br>`Router(config)# card type e1 0/3` | Sets the serial mode for the interface module:<br>• t1—Specifies T1 connectivity of 1.536 Mbps. B8ZS is the default linecode for T1.<br>• e1—Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 1.984 Mbps in framed mode and 2.048 Mbps in unframed E1 mode.<br>• *slot subslot* —Specifies the location of the interface module. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits configuration mode and returns to the EXEC command interpreter prompt. |

### Enabling T1 Controller

**Note** T1/T3 or E1/E3 does not require any license.

To enable T1 controller:

```
enable
configure terminal
controller mediatype 0/4/0
mode t1
end
```

## Configuring the Controller

To create the interfaces for the T1/E1 interface module, complete these steps:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **controller** {**t1** \| **e1**} *slot/subslot/port*<br>**Example:**<br>`Router(config)# controller t1 0/3/0` | Selects the controller to configure and enters controller configuration mode.<br>• t1—Specifies the T1 controller.<br>• e1—Specifies the E1 controller.<br>• *slot/subslot/port*—Specifies the location of the interface.<br>**Note** The slot number is always 0. |
| **Step 3** | **clock source** {**internal** \| **line**}<br>**Example:**<br>`Router(config-controller)# clock source internal` | Sets the clock source.<br>**Note** The clock source is set to internal if the opposite end of the connection is set to line and the clock source is set to line if the opposite end of the connection is set to internal.<br>• internal—Specifies that the internal clock source is used. |

| | Command or Action | Purpose |
|---|---|---|
| | | • line—Specifies that the network clock source is used. This is the default for T1 and E1. |
| **Step 4** | **linecode** {**ami** \| **b8zs** \| **hdb3**}<br>**Example:**<br>`Router(config-controller)# linecode ami` | Selects the linecode type.<br>• ami—Specifies Alternate Mark Inversion (AMI) as the linecode type. Valid for T1 and E1 controllers.<br>• b8zs—Specifies binary 8-zero substitution (B8ZS) as the linecode type. Valid for T1 controller only. This is the default for T1 lines.<br>• hdb3—Specifies high-density binary 3 (HDB3) as the linecode type. Valid for E1 controller only. This is the default for E1 lines. |
| **Step 5** | For T1 Controllers:<br>**Example:**<br>`framing {sf \| esf}`<br>**Example:**<br>`Router(config-controller)# framing sf`<br>**Example:**<br>`For E1 Controllers:`<br>**Example:**<br>`framing {crc4 \| no-crc4}`<br>**Example:**<br>`Router(config-controller)# framing crc4` | Selects the framing type.<br>• sf—Specifies Super Frame as the T1 frame type.<br>• esf—Specifies Extended Super Frame as the T1 frame type. This is the default for E1.<br>• crc4—Specifies CRC4 as the E1 frame type. This is the default for E1.<br>• no-crc4—Specifies no CRC4 as the E1 frame type. |
| **Step 6** | **cablelength** {**long** \| **short**}<br>**Example:**<br>`Router(config-controller)# cablelength long` | To fine-tune the pulse of a signal at the receiver for an E1 cable, use the **cablelength** command in controller configuration mode. |
| **Step 7** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits configuration mode and returns to the EXEC command interpreter prompt. |

## Verifying Controller Configuration

To verify the controller configuration, use the show controllers command :

```
Router# show controllers t1 0/3/0 brief
T1 0/3/0 is up.
  Applique type is A900-IMA16D
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
  Data in current interval (230 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Total Data (last 24 hours)
     136 Line Code Violations, 63 Path Code Violations,
     0 Slip Secs, 6 Fr Loss Secs, 4 Line Err Secs, 0 Degraded Mins,
     7 Errored Secs, 1 Bursty Err Secs, 6 Severely Err Secs, 458 Unavail Secs
     2 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

# Optional Configurations

There are several standard, but optional, configurations that might be necessary to complete the configuration of your T1/E1 interface module.

## Configuring Framing

Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. To configure framing, use the following commands.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **controller** {**t1** \| **e1**} *slot/subslot/port*<br>**Example:**<br>`Router(config)# controller t1 0/3/0` | Selects the controller to configure.<br>• t1—Specifies the T1 controller.<br>• e1—Specifies the E1 controller.<br>• slot/subslot/port—Specifies the location of the controller.<br>**Note** The slot number is always 0. |
| **Step 3** | For T1 controllers<br>**Example:**<br>**framing** {**sf** \| **esf**} | Sets the framing on the interface.<br>• sf—Specifies Super Frame as the T1 frame type. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router(config-controller)# framing sf`<br>**Example:**<br>**Example:**<br>`For E1 controllers`<br>**Example:**<br>**framing** {**crc4** \| **no-crc4**}<br>**Example:**<br>`Router(config-controller)# framing crc4` | • esf—Specifies Extended Super Frame as the T1 frame type. This is the default for T1.<br>• crc4—Specifies CRC4 frame as the E1 frame type. This is the default for E1.<br>• no-crc4—Specifies no CRC4 as the E1 frame type. |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits configuration mode and returns to the EXEC command interpreter prompt. |

### Verifying Framing Configuration

Use the show controllers command to verify the framing configuration:

```
Router# show controllers t1 0/3/0 brief
T1 0/3/0 is up.
  Applique type is A900-IMA16D
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Soaking time: 3, Clearance time: 10
  AIS State:Clear  LOS State:Clear  LOF State:Clear
  Framing is ESF, Line Code is B8ZS
, Clock Source is Line.
  Data in current interval (740 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
  Total Data (last 24 hours)
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
     0 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

## Setting an IP Address

To set an IP address for the serial interface, complete these steps:

You can also set an IP address using an IMA or CEM configuration.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **interface serial** *0/subslot/port:channel-group*<br>**Example:**<br>`Router(config)# interface serial 0/0/1:0` | Selects the interface to configure from global configuration mode.<br>• *subslot*—**Specifies the subslot in which the T1/E1 interface module is installed.**<br>• *port* —Specifies the location of the controller. The port range for T1 and E1 is 1 to 16.<br>• *channel-group* —Specifies the channel group number configured on the controller. For example: interface serial 0/0/1:1. |
| **Step 2** | **ip address** *address mask*<br>**Example:**<br>`Router(config-if)# ip address 192.0.2.1 255.255.255.0` | Sets the IP address and subnet mask.<br>• *address* —Specify the IP address.<br>• *mask* —Specify the subnet mask. |
| **Step 3** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits configuration mode and returns to the EXEC command interpreter prompt. |

### What to do next

**Note** IPV4 routing protocols, such as *eigrp* , *ospf* , *bgp* , and *rip* , are supported on serial interfaces.

## Configuring Encapsulation

When traffic crosses a WAN link, the connection needs a Layer 2 protocol to encapsulate traffic.

**Note** L2TPv3 encapsulation is *not* supported.

To set the encapsulation method, use the following commands:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:** | |
| **Step 2** | **interface serial** *0/subslot/port:channel-group*<br>**Example:**<br>`Router(config)# interface serial 0/0/1:0`<br>**Example:** | Selects the interface to configure from global configuration mode.<br>• *subslot*—**Specifies the subslot in which the T1/E1 interface module is installed.**<br>• *port* —Specifies the location of the controller. The port range for T1 and E1 is 1 to 16.<br>• *channel-group* —Specifies the channel group number configured on the controller. For example: interface serial 0/0/1:1. |
| **Step 3** | **encapsulation** {**hdlc** \| **ppp**}<br>**Example:**<br>`Router(config-if)# encapsulation hdlc` | Set the encapsulation method on the interface.<br>• **hdlc**—High-Level Data Link Control (HDLC) protocol for a serial interface. This encapsulation method provides the synchronous framing and error detection functions of HDLC without windowing or retransmission. This is the default for synchronous serial interfaces.<br>• **ppp**—Described in RFC 1661, PPP encapsulates network layer protocol information over point-to-point links. |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits configuration mode and returns to the EXEC command interpreter prompt. |

## Verifying Encapsulation

Use the **show interfaces serial** command to verify encapsulation on the interface:

```
Router#  show  interfaces  serial
  0/0/1:0
Serial0/0/1:0 is up, line protocol is up
  Hardware is Multichannel T1
  MTU 1500 bytes, BW 1536 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC
, crc 16, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
60 packets input, 8197 bytes, 0 no buffer
Received 39 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
64 packets output, 8357 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions
```

## Configuring the CRC Size for T1 Interfaces

All T1/E1 serial interfaces use a 16-bit cyclic redundancy check (CRC) by default, but also support a 32-bit CRC. CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.

CRC-16, the most widely used CRC throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE 802 and as an option by some point-to-point transmission standards.

To set the length of the cyclic redundancy check (CRC) on a T1 interface, use these commands:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal`<br>**Example:** | Enters global configuration mode. |
| **Step 2** | **interface serial** *0/subslot/port:channel-group*<br>**Example:**<br>`Router(config)# interface serial 0/0/1:0`<br>**Example:** | Selects the interface to configure from global configuration mode.<br>• *number* —Specifies the location of the controller. The number range for T1 and E1 is 1 to 16.<br>• *channel-group* —Specifies the channel group number configured on the controller. For example: interface serial 0/1:1. |
| **Step 3** | **crc** {**16** \| **32**}<br>**Example:**<br>`Router(config-if)# crc 16` | Selects the CRC size in bits.<br>• 16—16-bit CRC. This is the default.<br>• 32—32-bit CRC.<br>**Note** Moving from CRC 16 to 32 bit (and vice-versa) is not supported. |
| **Step 4** | **exit**<br>**Example:** | Exits configuration mode and returns to the EXEC command interpreter prompt. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config)# exit` | |

### Verifying the CRC Size

Use the **show interfaces serial** command to verify the CRC size set on the interface:

```
Router#  show  interfaces  serial  0/0/1:0
Serial0/0/1:0 is up, line protocol is up
  Hardware is Multichannel T1
  MTU 1500 bytes, BW 1536 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16
, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     60 packets input, 8197 bytes, 0 no buffer
     Received 39 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     64 packets output, 8357 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
```

## Configuring a Channel Group

Follow these steps to configure a channel group:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **controller** {**t1** \| **e1**} *slot/subslot/port*<br>**Example:**<br>`Router(config)# controller t1 0/3/0` | Select the controller to configure and enter global configuration mode. |
| **Step 3** | **channel-group** [**t1** \| **e1**] *number* {**timeslots** *range* \| **unframed**} [**speed** {**56** \| **64**}]<br>**Example:** | Defines the time slots that belong to each T1 or E1 circuit.<br>• *number*— Channel-group number. When configuring a T1 data line, channel-group |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config-controller)# channel-group t1 1timeslots 1 \| unframed speed 56` | numbers can be values from 1 to 28. When configuring an E1 data line, channel-group numbers can be values from 0 to 30.<br>• **timeslots** *range*— One or more time slots or ranges of time slots belonging to the channel group. The first time slot is numbered 1. For a T1 controller, the time slot range is from 1 to 24. For an E1 controller, the time slot range is from 1 to 31.<br>• **unframed**—Unframed mode (G.703) uses all 32 time slots for data. None of the 32 time slots are used for framing signals.<br>• **speed**—(Optional) Specifies the speed of the underlying DS0s in kilobits per second. Valid values are 56 and 64.<br>**Note** The default is 64. Speed is not mentioned in the configuration.<br>**Note** Each channel group is presented to the system as a serial interface that can be configured individually.<br>**Note** Once a channel group has been created with the channel-group command, the channel group cannot be changed without removing the channel group. To remove a channel group, use the **no** form of the **channel-group** command.<br>**Note** The unframed option is not currently supported.<br>**Note** DS0-level channelization is not currently supported. |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config)# exit` | Exits configuration mode and returns to the EXEC command interpreter prompt. |

## Saving the Configuration

To save your running configuration to nonvolatile random-access memory (NVRAM), use the following command in privileged EXEC configuration mode:

| Command | Purpose |
|---|---|
| **copy running-config startup-config** | Writes the new configuration to NVRAM. |

For information about managing your system images and configuration files, refer to the Cisco IOS Configuration Fundamentals Configuration Guide and Cisco IOS Configuration Fundamentals Command Reference publications.

# Troubleshooting E1 and T1 Controllers

You can use the following methods to troubleshoot the E1 and T1 controllers using Cisco IOS software:


- Setting Loopbacks, on page 126
- Runing Bit Error Rate Testing, on page 127


## Setting Loopbacks

The following sections describe how to set loopbacks:

### Setting a Loopback on the E1 Controller

To set a loopback on the E1 controller, perform the first task followed by any of the following tasks beginning in global configuration mode:

| Command | Purpose |
|---|---|
| **configure terminal** | Enters global configuration mode. |
| **controller e1** *slot/subslot/port* | Select the E1 controller and enter controller configuration mode.The slot number is always 0. |
| **loopback diag** | Set a diagnostic loopback on the E1 line. |
| **loopback network** {**line** \| **payload**} | Set a network payload loopback on the E1 line. |
| **end** | Exit configuration mode when you have finished configuring the controller. |

### Setting a Loopback on the T1 Controller

You can use the following loopback commands on the T1 controller in global configuration mode:

| Task | Command |
|---|---|
| **controller t1** *slot/subslot/port* | Selects the T1 controller and enter controller configuration mode<br>The slot number is always 0. |
| **loopback diag** | Sets a diagnostic loopback on the T1 line. |
| **loopback local** {**line** \| **payload**} | Sets a local loopback on the T1 line. You can select to loopback the line or the payload. |
| **loopback remote iboc** | Sets a remote loopback on the T1 line. This loopback setting will loopback the far end at line or payload, using IBOC (in band bit-orientated code) or the Extended Super Frame (ESF) loopback codes to communicate the request to the far end. |
| **end** | Exits configuration mode when you have finished configuring the controller. |

**Note** To remove a loopback, use the **no loopback** command.

*Table 13: Loopback Descriptions*

| Loopback | Description |
|---|---|
| **loopback diag** | Loops the outgoing transmit signal back to the receive signal. This is done using the diagnostic loopback feature in the interface module's PMC framer. The interface module transmits AIS in this mode. Set the **clock source** command to **internal** for this loopback mode. |
| **loopback local** | Loops the incoming receive signal back out to the transmitter. You can specify whether to use the **line** or **payload**. |
| **local line** | The incoming signal is looped back in the interface module using the framer's line loopback mode. The framer does not reclock or reframe the incoming data. All incoming data is received by the interface module driver. |
| **local payload** | Loops the incoming signal back in the interface module using the payload loopback mode of the framer. The framer reclocks and reframes the incoming data before sending it back out to the network. When in payload loopback mode, an all 1s data pattern is received by the local HDLC receiver and the clock source is automatically set to line (overriding the **clock source** command). When the payload loopback is ended, the clock source returns to the last setting selected by the **clock source** command. |
| **loopback remote iboc** | Attempts to set the far-end T1 interface into line loopback. This command sends an in-band bit-oriented code to the far-end to cause it to go into line loopback. This command is available when using ESF or SF framing mode. |
| **network line** | Loops the incoming signal back in the interface module using the line loopback mode of the framer. The framer does not reclock or reframe the incoming data. All incoming data is received by the interface module driver. |
| **network payload** | Loops the incoming signal back using the payload loopback mode of the framer. The framer reclocks and reframes the incoming data before sending it back out to the network. When in payload loopback mode, an all 1s data pattern is received by the local HDLC receiver, and the clock source is automatically set to line (overriding the **clock source** command). When the payload loopback is ended, the clock source returns to the last setting selected by the **clock source** command. |

# Runing Bit Error Rate Testing

Bit error rate testing (BERT) is supported on each of the E1 or T1 links. The BERT testing is done only over a framed E1 or T1 signal and can be run only on one port at a time.

The interface modules contain onboard BERT circuitry. With this, the interface module software can send and detect a programmable pattern that is compliant with CCITT/ITU O.151, O.152, and O.153 pseudo-random and repetitive test patterns. BERTs allows you to test cables and signal problems in the field.

When running a BER test, your system expects to receive the same pattern that it is transmitting. To help ensure this, two common options are available:

- Use a loopback somewhere in the link or network
- Configure remote testing equipment to transmit the same BERT test pattern at the same time

To run a BERT on an E1 or T1 controller, perform the following optional tasks beginning in global configuration mode:

| Task | Command |
|---|---|
| **controller** {**e1** \| **t1**} *slot/subslot/port* | Selects the E1 or T1 controller and enters controller configuration mode.<br>The slot number is always 0. |
| **bert pattern 0s** \| **1s** \| **2^11** \| **2^15** \| **2^20-O153** \| **2^20-QRSS** \| **2^23** \| **alt-0-1**} **interval** *minutes* | Specifies the BERT pattern for the E1 or T1 line and the duration of the test in minutes. The valid range is 1 to 1440 minutes.<br>**Note** Only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported. |
| **end** | Exit configuration mode when you have finished configuring the controller. |
| **show controllers** {**e1** \| **t1**} *slot/subslot/port* | Displays the BERT results. |

The following keywords list different BERT keywords and their descriptions.

**Caution** Currently only the 2^11, 2^15, 2^20-O153, and 2^20-QRSS patterns are supported.

***Table 14: BERT Pattern Descriptions***

| Keyword | Description |
|---|---|
| **0s** | Repeating pattern of zeros (...000...). |
| **1s** | Repeating pattern of ones (...111...). |
| **2^11** | Pseudo-random test pattern that is 2,048 bits in length. |
| **2^15** | Pseudo-random O.151 test pattern that is 32,768 bits in length. |
| **2^20-O153** | Pseudo-random O.153 test pattern that is 1,048,575 bits in length. |
| **2^20-QRSS** | Pseudo-random QRSS O.151 test pattern that is 1,048,575 bits in length. |
| **2^23** | Pseudo-random 0.151 test pattern that is 8,388,607 bits in length. |

| Keyword | Description |
| --- | --- |
| **alt-0-1** | Repeating alternating pattern of zeros and ones (...01010...). |

Both the total number of error bits received and the total number of bits received are available for analysis. You can select the testing period from 1 minute to 24 hours, and you can also retrieve the error statistics anytime during the BER test.

**Note** To terminate a BERT test during the specified test period, use the **no bert** command.

You can view the results of a BERT test at the following times:

- After you terminate the test using the **no bert** command
- After the test runs completely
- Anytime during the test (in real time)

# Monitoring and Maintaining the T1/E1 Interface Module

After configuring the new interface, you can monitor the status and maintain the interface module by using **show** commands. To display the status of any interface, complete any of the following tasks in **EXEC** mode:

| Task | Command |
| --- | --- |
| **show controllers** {**e1** \| **t1**} [*slot/port-adapter/port/e1-line*] [**brief** | Displays the status of the E1 or T1 controller. |
| **show interface serial***slot/subslot/port* | Displays statistics about the serial information for a specific E1 or T1 channel group. Valid values are 0 to 30 for E1 and 0 to 23 for T1. |
| **clear counters serial** *slot/subslot/port* | Clears the interface counters |

**Note** To change the T1/E1 card type configuration, use the **no card type** command and reload the router.

# AIS on Core Failure

AIS stands for Alarm Indication Signal. Prior to Cisco IOS XE Fuji Release 16.7.1, the PDH AIS alarms were generated only when the CE would go down and an event was set in the CEM control-word by the remote provider edge (PE). AIS alarms were not generated when the pesudowire went down. Now, AIS alarm are generated when the pesudowire goes down.

This feature is only supported on the Cisco ASR 900 RSP2 module, for 8-port T1/E1 and 16-port T1/E1 interface modules and only for unframed E1 mode (SAToP) type.

## Limitations of AIS

- AIS is not supported on CESoP and CEM over UDP.
- AIS is not supported on T1 mode. It is only supported on E1 mode.
- AIS is not supported on the 4-port OC3/STM-1 (OC-3) interface module (IM) and 32-port T1/E1 IM.
- AIS is supported only for MPLS core.
- AIS is not supported in pseudowire HSPW mode, when **graceful-restart** command is enabled.
- Removing the MPLS IP address from the core interfaces results in a delay of 10-12 minutes to notify the peer end. This depends on the negotiated forwarding hold timer between the routers, which is the least value of the configured LDP GR forwarding hold timer of the two routers.
- Supported CEM class range of de-jitter buffer size is between 1 to 32 ms.
- If the **shutdown unpowered** command is used to shut down the IM, an OIR must be performed to trigger the AIS alarms..

## Core Failure Event Detection

AIS configuration is used to detect core defects. The core failure is detected in the following events:

- Shutdown of the PE controller or tug level.
- Removing the cross-connect feature.
- Removal of Gigabit Ethernet configuration, CEM configuration, controller configuration, or OSPF configuration.
- Shut on OSPF, CEM group, cross-connect, or Gigabit Ethernet interface.
- CE1 controller shut—AIS alarm is seen on the remote CE.
- PE1 controller shut—AIS alarm is seen on the remote CE.
- PE1 core shut—AIS alarm is seen on both the CEs.
- PE2 core shut—AIS alarm is seen on both the CEs.
- Pesudowire down—AIS alarm is seen on both the CEs.
- Core IGP down—AIS alarm is seen on both the CEs.
- Core LDP down—AIS alarm is seen on both the CEs.

## Configuring AIS for Core Failure

When you enable the AIS, Plesiochronous Digital Hierarchy (PDH) AIS alarm is supported for core failure events on the 8-port T1/E1 and 16-port T1/E1 interface modules. When a core failure is detected due to any event, core flap flag is updated and the core flap event sends an event, which asserts an AIS. When the AIS is not enabled, core failure events are ignored.

Use the following procedure to enable AIS:

```
Router> enable
Router#configure terminal
```

```
Router(config)#controller t1 0/1/2
Router(config-controller)#ais-core-failure
```

### Verifying AIS Configuration

Use the **show run | sec** command to verify the configuration of AIS:

```
Router(config-controller)#show run | sec 0/3/0
controller E1 0/3/0
 ais-core-failure
 framing unframed
  cem-group 30 unframed
interface CEM0/3/0
```

### Example: AIS Trigger

The following example shows a sample configuration of a controller O/P when an AIS is triggered:

```
Router#show controller e1 0/2/1
E1 0/2/1 is down.
Applique type is A900-IMA16D
Cablelength is Unknown
Transmitter is sending remote alarm.
Receiver is getting AIS. <<<<<<<<<<<<< This is AIS alarm received
ais-shut is not set
alarm-trigger is not set
Framing is crc4, Line Code is HDB3, Clock Source is Line.
BER thresholds: SF = 10e-5 SD = 10e-5
International Bit: 1, National Bits: 11111
Data in current interval (0 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
1 Near-end path failures, 0 Far-end path failures, 0 SEF/AIS Secs
```

# Verifying the Interface Configuration

Besides using the **show running-configuration** command to display the configuration settings, use the **show interfaces serial** and the **show controllers serial** commands to get detailed information on a per-port basis for your T1/E1 interface module.

## Verifying Per-Port Interface Status

To view detailed interface information on a per-port basis for the T1/E1 interface module, use the **show interfaces serial** command.

```
Router# show interfaces serial 0/0/1:0
Serial0/0/1:0 is up, line protocol is up
  Hardware is SPA-8XCHT1/E1
  Internet address is 79.1.1.2/16
  MTU 1500 bytes, BW 1984 Kbit, DLY 20000 usec,
     reliability 255/255, txload 240/255, rxload 224/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive not set
  Last input 3d21h, output 3d21h, output hang never
  Last clearing of ''show interface'' counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 2998712
```

```
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 1744000 bits/sec, 644 packets/sec
  5 minute output rate 1874000 bits/sec, 690 packets/sec
     180817311 packets input, 61438815508 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
     180845200 packets output, 61438125092 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions no alarm present
  Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags 2
```

# Configuration Examples

This section includes the following configuration examples:

## Example: Framing and Encapsulation Configuration

The following example sets the framing and encapsulation for the controller and interface:

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 2/0/0
!
! Specify the framing method
!
Router(config-controller)# framing esf
!
! Exit controller configuration mode and return to global configuration mode
!
Router(config-controller)# exit
!
! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 2/0/0:0
!
! Specify the encapsulation protocol
!
Router(config-if)# encapsulation ppp
!
! Exit interface configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

## Example: CRC Configuration

The following example sets the CRC size for the interface:

```
! Specify the interface and enter interface configuration mode
!
Router(config)# interface serial 2/0/0:0
```

```
!
! Specify the CRC size
!
Router(config-if)# crc 32
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

# Example: Facility Data Link Configuration

The following example configures Facility Data Link:

```
! Specify the controller and enter controller configuration mode
!
Router(config)# controller t1 2/0/0
!
! Specify the FDL specification
!
Router(config-controller)#
fdl ansi
!
! Exit controller configuration mode and return to global configuration mode
!
Router(config-controller)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

# Example: Invert Data on the T1/E1 Interface

The following example inverts the data on the serial interface:

```
! Enter global configuration mode
!
Router# configure terminal
!
! Specify the serial interface and enter interface configuration mode
!
Router(config)# interface serial 2/1/3:0
!
! Configure invert data
!
Router(config-if)# invert data
!
! Exit interface configuration mode and return to global configuration mode
!
Router(config-if)# exit
!
! Exit global configuration mode
!
Router(config)# exit
```

CHAPTER 8

# Dying Gasp Support for Loss of Power Supply via SNMP, Syslog and Ethernet OAM

Dying Gasp—One of the following unrecoverable condition has occurred:

- Interface error-disable
- Reload
- Power failure or removal of power supply cable

This type of condition is vendor specific. An Ethernet Operations, Administration, and Maintenance (OAM) notification about the condition may be sent immediately.



## Prerequisites for Dying Gasp Support

Dying Gasp via ethernet OAM is not supported on Cisco RSP3 module.

You must enable Ethernet OAM on interface that requires Dying Gasp notification via Ethernet OAM. For more information, see *Enabling Ethernet OAM on an interface*.

You must enable SNMP global configurations to get notification via SNMP trap. For more information, see *Configuration Examples for Dying Gasp support via SNMP*.

## Restrictions for Dying Gasp Support

- The Dying Gasp feature is not supported if you remove the power supply unit (PSU) from the system.
- SNMP trap is sent only on power failure that results in the device to shut down.
- The Dying Gasp support feature cannot be configured using CLI. To configure hosts using SNMP, refer to the SNMP host configuration examples below.

- Dying Gasp via SNMP Trap is *not* supported on Management Port Gig0/Management-interface vrf on Cisco RSP3 module and Cisco ASR 920 routers.

# Configuration Examples for Dying Gasp Support

## Configuring SNMP Community Strings on a Router

Setting up the community access string to permit access to the SNMP:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server community public RW
Router(config)# exit
```

For more information on command syntax and examples, refer to the Cisco IOS Network Management Command Reference.

## Configuring SNMP-Server Host Details on the Router Console

Specifying the recipient of a SNMP notification operation:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host X.X.X.XXX vrf mgmt-intf version 2c public udp-port 9800
```

Router(config)# exit

For more information on command syntax and examples, refer to the Cisco IOS Network Management Command Reference.

# Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations

**Note** You can configure up to five different SNMP server host/port configurations.

## Environmental Settings on the Network Management Server

```
setenv SR_TRAP_TEST_PORT=UDP port
setenv SR_UTIL_COMMUNITY=public
setenv SR_UTIL_SNMP_VERSION=v2c
setenv SR_MGR_CONF_DIR=Path to the executable snmpinfo.DAT file
```

The following example shows SNMP trap configuration on three hosts:

Configuration example for the first host:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)# snmp-server host 7.0.0.149 vrf Mgmt-intf version 2c public udp-port 6264
Configuration example for the second host:
Router(config)#
Router(config)# snmp-server host 7.0.0.152 vrf Mgmt-intf version 2c public udp-port 9988
Configuration example for the third host:
Router(config)# snmp-server host 7.0.0.166 vrf Mgmt-intf version 2c public udp-port 9800
Router(config)#
Router(config)# ^Z
Router#
```

After performing a power cycle, the following output is displayed on the router console:

**Note** This is not supported on Cisco RSP1 and Cisco RSP2 modules.

```
Router#
System Bootstrap, Version 15.3(2r)S, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012 by cisco Systems, Inc.
Compiled Wed 17-Oct-12 15:00
Current image running: Boot ROM1
Last reset cause: PowerOn
UEA platform with 2097152 Kbytes of main memory
rommon 1 >
=======================================
Dying Gasp Trap Received for the Power failure event:
-----------------------------------------------------
  Trap on Host1
++++++++++++++
snmp-server host = 7.0.0.149 (nms1-lnx)  and SR_TRAP_TEST_PORT=6264
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
--------------------------------------------------------------------
  Trap on Host2
+++++++++++++
snmp-server host = 7.0.0.152  (nms2-lnx)  and SR_TRAP_TEST_PORT=9988
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
--------------------------------------------------------------
   Trap on Host3
++++++++++++++
snmp-server host = 7.0.0.166  (erbusnmp-dc-lnx)  and SR_TRAP_TEST_PORT=9800
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 7.29.25.101
```

```
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
```

# Message Displayed on the Peer Router on Receiving Dying Gasp Notification

```
001689: *May 30 14:16:47.746 IST: %ETHERNET_OAM-6-RFI: The client on interface Gi4/2 has
received a remote failure indication from its remote peer(failure reason = remote client
power failure action = )
```

# Displaying SNMP Configuration for Receiving Dying Gasp Notification

Use the show running-config command to display the SNMP configuration for receiving dying gasp notification:

```
Router# show running-config | i snmp
snmp-server community public RW
snmp-server host 7.0.0.149 vrf Mgmt-intf version 2c public udp-port 6264
snmp-server host 7.0.0.152 vrf Mgmt-intf version 2c public udp-port 9988
snmp-server host 7.0.0.166 vrf Mgmt-intf version 2c public udp-port 9800
Router#
```

# Dying GASP via SNMP Trap Support on Cisco RSP3 Module

Dying GASP via SNMP trap feature is supported on Cisco RSP3 module.

no packets can be processed in this time by CPU. To avoid this, this feature pre-constructs and installs the event packet in FPGA. When FPGA receives the power failure notificaion, it transfers the pre-constructed packet and thus the packet is forwarded to the required egress interface.

The feature helps to quickly notify a network administrator whenever a node undergoes power shutdown. The node undergoing power shutdown sends a SNMP DG trap message to the configured SNMP server .

The feature is supported on global MPLS and L3VPN. It uses UDP port 49151 as source port and 162 as destination port.

## Restrictions for Dying GASP via SNMP Trap Support on Cisco RSP3 Module

- The feature is enabled by default in Cisco RSP3C Port Expansion Mode when the channelized IMs are inserted in the device with the following conditions:

  If the above-mentioned IMs are not inserted in the above-mentioned slots, you can still connect by enabling the following command in the global configurations:

  **platform dying-gasp-port-enable**

**Note** The above command only supported in Cisco RSP3C Port Expansion Mode.

But, some IMs in some slot can no longer be online. The enabled command checks if these slots are free of those IMs, if they are not, it rejects the implementation and error message is displayed. The same scenario is experienced when the command is enabled and incompatible IM is inserted. For information on incompatible IMs, refer the IM Compatibility Tool .

- Only SNMP Dying Gasp traps are received in an event of power failure.

  The SNMP Dying Gasp traps are *only* received for the first five configured SNMP hosts. Only five SNMP server hosts are notified about SNMP trap.

- Generation of SNMP trap for host via management VRF for a Dying GASP event is not supported in Cisco RSP3 Module.
- Reachability to the host must be present and Address Resolution Protocol (ARP) must be resolved before the event.
- Dying GASP support for loss of power supply via syslog and Ethernet OAM is not supported.

# Enabling Dying GASP Support on Cisco RSP3 Module

To enable Dying GASP feature for Cisco RSP3 module in Cisco RSP3C Port Expansion Mode:

```
enable
configure terminal
platform dying-gasp-port-enable
end
```

To enable the feature in Cisco RSP3C XFI-Pass Through Mode:

```
enable
configure terminal
license feature service-offload enable
Reload the device. If present, IM  goes out of serive. If not, deactivate the IM.
license feature service-offload bandwidth 10gbps npu-[0 | 1]
Reload the device.
end
```

# Verifying SNMP Host Configuration

Use **show snmp host** command to verify all SNMP hosts configured.

```
#show snmp host
Notification host: 20.20.20.21  udp-port: 162   type: trap
user: public    security model: v2c

Notification host: 30.30.30.31  udp-port: 162   type: trap
user: public    security model: v2c

Notification host: 5000::2      udp-port: 162   VRFName: vrf1   type: trap
user: public    security model: v3 noauth

Notification host: 6000::2      udp-port: 162   VRFName: vrf1   type: trap
user: public    security model: v3 noauth
```

```
Notification host: 8000::2      udp-port: 162   type: trap
user: public    security model: v2c
```

# Verifying SNMP Configurations

Use **show running | i snmp** command to verify all SNMP hosts configured.

```
#show running | i snmp
snmp-server group public v3 noauth
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source Loopback0
snmp-server host 20.20.20.21 version 2c public
snmp-server host 30.30.30.31 version 2c public
snmp-server host 5000::2 vrf vrf1 version 3 noauth public
snmp-server host 6000::2 vrf vrf1 version 3 noauth public
snmp-server host 8000::2 version 2c public
```

CHAPTER 9

# Configuring the Global Navigation Satellite System

The chassis uses a satellite receiver, also called the global navigation satellite system (GNSS), as a new timing interface.

In typical telecom networks, synchronization works in a hierarchal manner where the core network is connected to a stratum-1 clock and this clock is then distributed along the network in a tree-like structure. However, with a GNSS receiver, clocking is changed to a flat architecture where access networks can directly take clock from satellites in sky using an on-board GPS chips.

This capability simplifies network synchronization planning, provides flexibility and resilience in resolving network synchronization issues in the hierarchical network.



## Information About the GNSS

### Overview of the GNSS Module

The GNSS module is present on the front panel of the RSP3 module and can be ordered separately with PID=. However, there is no license required to enable the GNSS module.

The GNSS LED on the RSP3 front panel indicates the status of the module. The following table explains the different LED status.

| LED Status | Description |
|---|---|
| Green | GNSS Normal State. Self survey is complete. |
| Amber | All other states |

When connected to an external antenna, the module can acquire satellite signals and track up to 32 GNSS satellites, and compute location, speed, heading, and time. GNSS provides an accurate one pulse-per-second

(PPS), a stable 10 MHz frequency output to synchronize broadband wireless, aggregation and pre-aggregation routers, and an accurate time-of-day (ToD).

> **Note** The RSP3 module can also receive 1PPS, 10 MHz, and ToD signals from an external clocking and timing source. However, the timing signals from the GNSS module (when enabled) take precedence over those of the external source.

By default, anti-jamming is enabled on the GNSS module.

# Operation of the GNSS Module

The GNSS module has the following stages of acquiring and providing timing signals to the Cisco router:

- Self-Survey Mode—When the router is reset, the GNSS module comes up in self-survey mode. It tries to lock on to minimum four different satellites and computes approximately 2000 different positions of the satellites to obtain a 3-D location (Latitude, Longitude, and Height) of it current position. This operation takes about 35-to-40 minutes. During this stage also, the module is able to generate accurate timing signals and achieve a *Normal* or *Phase-locked* state.

When GNSS moves into *Normal* state, you can start using the 1PPS, 10 MHz, and ToD inputs from GNSS. The quality of the signal in Self-Survey mode with *Normal* state is considered good enough to lock to GNSS.

- Over determined clock mode—The router switches to over determined (OD) mode when the self-survey mode is complete and the position information is stored in non-volatile memory on the router. In this mode, the module only processes the timing information based on satellite positions captured in self-survey mode.

The router saves the tracking data, which is retained even when the router is reloaded. If you want to change the tracking data, use the **no shutdown** command to set the GNSS interface to its default value.

The GNSS module stays in the OD mode unless one of the following conditions occur:

- A position relocation of the antenna of more than 100 meters is detected. This detection causes an automatic restart of the self-survey mode.
- A manual restart of the self-survey mode or when the stored reference position is deleted.
- A worst-case recovery option after a jamming-detection condition that cannot be resolved with other methods.

You can configure the GNSS module to automatically track any satellite or configure it to explicitly use a specific constellation. However, the module uses configured satellites only in the OD mode.

> **Note** GLONASS and BeiDou satellites cannot be enabled simultaneously. GALILEO is not supported.

When the router is reloaded, it always comes up in the OD mode unless:

- the router is reloaded when the Self-Survey mode is in progress
- the physical location of the router is changed to more than 100 m from it’s pre-reloaded condition.

When the GNSS self-survey is restarted using the default **gnss slot R0/R1** command in config mode, the 10MHz, 1PPS, and ToD signals are not changed and remain up.

## Anti-Jamming

By default, anti-jamming is enabled on the GNSS module.

## High Availability for GNSS

The chassis has two GNSS modules, one each on the active and standby RSP3 modules. Each GNSS module must have a separate connection to the antenna in case of an RSP3 switchover.

## Prerequisites for GNSS

To use GNSS:

- 1PPS, 10 MHz, and ToD must be configured for netsync and PTP. For more information see the Configuring Clocking and Timing chapter .
- The antenna must have a clear view of the sky. For proper timing, minimum of four satellites should be locked. For information, see the *Cisco NCS 4206 Series Hardware Installation Guide* .

## Restrictions for GNSS

- The GNSS module is not supported through SNMP; all configurations are performed through commands.
- On HA system, the traps from the standby system are logged to the console as the SNMP infra does not get enabled on standby RSP module.
- GNSS objects or performance counters are updated every 5 seconds locally and acknowledge the MIB object request accordingly.
- GNSS traps generation is delayed for 300 seconds for the first time after system startes to avoid any drop of GNSS traps.

# How to Configure the GNSS

**Note** To know more about the commands referenced in this document, see the Cisco IOS Master Command List .

## Enabling the GNSS License

```
enable
configure terminal
license feature gnss
exit
```

# Enabling the GNSS on the Cisco Router

```
enable
configure terminal
gnss slot r0
no shutdown
exit
```

**Note** After the GNSS module is enabled, GNSS will be the source for 1PPS, ToD, and 10MHz clocking functions.

# Configuring the Satellite Constellation for GNSS

```
enable
configure terminal
gnss slot r0
constellation [auto | gps | galelio | beidou | qzss
exit
```

# Configuring Pulse Polarity

```
enable
configure terminal
gnss slot r0
1pps polarity negative
exit
```

**Note** The **no 1pps polarity negative** command returns the GNSS to default mode (positive is the default value).

# Configuring Cable Delay

```
enable
configure terminal
gnss slot r0
1pps offset 5
exit
```

**Note** It is recommended to compensate 5 nanosecond per meter of the cable.

The **no 1pps offset** command sets cable delay offset to zero.

# Disabling Anti-Jam Configuration

```
enable
configure terminal
gnss slot

ro
anti-jam disable
exit
```

# Verifying the Configuration of the GNSS

Use the **show gnss status** command to display status of GNSS.

```
Router# show gnss status
GNSS status:

  GNSS device: detected
  Lock status: Normal
  Receiver Status: Auto
  Clock Progress: Phase Locking
  Survey progress: 100
  Satellite count: 22
  Holdover Duration: 0
  PDOP: 1.04   TDOP: 1.00
  HDOP: 0.73   VDOP: 0.74
  Minor Alarm: NONE
  Major Alarm: None
```

Use the **show gnss satellite** command to display the status of all satellite vehicles that are tracked by the GNSS module.

```
Router# show gnss satellite all
All Satellites Info:

SV PRN No   Channel No       Acq Flg    Ephemeris Flg     SV Type     Sig Strength
----------------------------------------------------------------------------------
14          0                      1                1           0               47
21          2                      1                1           0               47
22          3                      1                1           0               46
18          4                      1                1           0               47
27          6                      1                1           0               44
31          8                      1                1           0               49
24          10                     1                1           0               42
79          12                     0                1           1               18
78          13                     1                1           1               26

Router# show gnss satellite 21
Selected Satellite Info:

  SV PRN No: 21
  Channel No: 2
  Acquisition Flag: 1
 Ephemeris Flag: 1
  SV Type: 0
  Signal Strength: 47
```

```
Router# show gnss time

Current GNSS Time:

  Time: 2015/10/14  12:31:01 UTC Offset: 17

Router# show gnss location
Current GNSS Location:

  LOC: 12:56.184000 N  77:41.768000 E 814.20 m
```

Use the **show gnss device** to displays the hardware information of the active GNSS module.

```
Router# show gnss device
GNSS device:

  Serial number: FOC2130ND5X
  Firmware version: 1.4
  Firmware update progress: NA
  Authentication: Passed
```

## Swapping the GNSS Module

Hot swap is supported on the RSP3 module of the GNSS.

1. Remove the standby RSP module.
2. Replace the GNSS module on the standby RSP slot.
3. Reinsert the RSP into the chassis and wait for the RSP to boot with standby ready.
4. Check for GNSS Lock Status of the standby RSP. Use command **show platform hardware slot** *<R0/R1>* [**network-clocks** | **sec GNSS**] to verify.
5. Trigger SSO after the GNSS on standby RSP is locked.
6. Repeat steps 1–3 for the other RSP.

# Configuration Example For Configuring GNSS

```
gnss slot R0
no shutdown
anti-jam disable
constellation glonass
1pps polarity negative
1pps offset 1000 negative
```

# Additional References

### Standards

| Standard | Title |
|---|---|
| — | There are no associated standards for this feature, |

### MIBs

| MIB | MIBs Link |
|---|---|
| • There are no MIBs for this feature. | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| — | There are no associated RFCs for this feature. |

CHAPTER 10

# G.8275.1 Telecom Profile

First Published: March 29, 2016

Precision Time Protocol (PTP) is a protocol for distributing precise time and frequency over packet networks. PTP is defined in the IEEE Standard 1588. It defines an exchange of timed messages

PTP allows for separate profiles to be defined in order to adapt PTP for use in different scenarios. A profile is a specific selection of PTP configuration options that are selected to meet the requirements of a particular application.

This recommendation allows for proper network operation for phase and time synchronization distribution when network equipment embedding a telecom boundary clock (T-BC) and a telecom time subordinate clock (T-TSC) is timed from another T-BC or a telecom grandmaster clock (T-GM). This recommendation addresses only the distribution of phase and time synchronization with the full timing support architecture as defined in ITU-T G.8275.



# Why G.8275.1?

The G.8275.1 profile is used in mobile cellular systems that require accurate synchronization of time and phase. For example, the fourth generation (4G) of mobile telecommunications technology.

The G.8275.1 profile is also used in telecom networks where phase or time-of-day synchronization is required and where each network device participates in the PTP protocol.

Because a boundary clock is used at every node in the chain between PTP Grandmaster and PTP Subordinate, there is reduction in time error accumulation through the network.

## More About G.8275.1

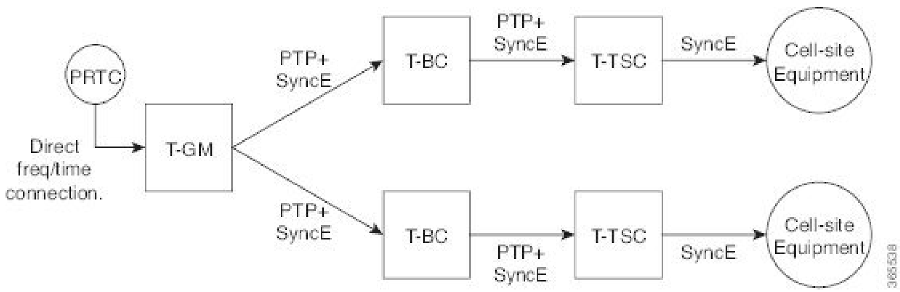
The G.8275.1 must meet the following requirements:

- Non-participant devices, that is, devices that only forward PTP packets, and PTP transparent clocks are not allowed.

- The telecom grandmaster (T-GM) provides timing to all other devices on the network. It does not synchronize its local clock with any other network element other than the Primary Reference Time Clock (PRTC).
- The telecom time subordinate clock (T-TSC) synchronizes its local clock to another PTP clock (in most cases, the T-BC), and does not provide synchronization through PTP to any other device.
- The telecom boundary clock (T-BC) synchronizes its local clock to a T-GM or an upstream T-BC, and provides timing information to downstream T-BCs or T-TSCs. If at a given point in time there are no higher-quality clocks available to a T-BC to synchronize to, it may act as a grandmaster.

The following figure describes a sample G.8275.1 topology.

***Figure 4: A Sample G.8275.1 Topology***




## PTP Domain

A PTP domain is a logical grouping of clocks that communicate with each other using the PTP protocol.

A single computer network can have multiple PTP domains operating separately, for example, one set of clocks synchronized to one time scale and another set of clocks synchronized to another time scale. PTP can run over either Ethernet or IP, so a domain can correspond to a local area network or it can extend across a wide area network.

The allowed domain numbers of PTP domains within a G.8275.1 network are between 24 and 43 (both inclusive).

## PTP Messages and Transport

The following PTP transport parameters are defined:

- For transmitting PTP packets, either the forwardable multicast MAC address (01-1B-19-00-00-00) or the non-forwardable multicast MAC address (01-80-C2-00-00-0E) must be used as the destination MAC address. The MAC address in use is selected on a per-port basis through the configuration. However, the non-forwardable multicast MAC address (01-80-C2-00-00-0E) will be used if no destination MAC is configured.

The source MAC address is the interface MAC address.

- For receiving PTP packets, both multicast MAC addresses (01-80-C2-00-00-0E and 01-1B-19-00-00-00) are supported.
- The packet rate for Announce messages is 8 packets-per-second. For Sync, Delay-Req, and Delay-Resp messages, the rate is 16 packets-per-second.
- Signaling and management messages are not used.

## PTP Modes

**Two-Way Operation**

To transport phase and time synchronization and to measure propagation delay, PTP operation must be two-way in this profile. Therefore, only two-way operation is allowed in this profile.

**One-Step and Two-Step Clock Mode**

Both one-step and two-step clock modes are supported in the G.8275.1 profile.

A client port must be capable of receiving and processing messages from both one-step clocks and two-step clocks, without any particular configuration. However, the server clock supports only one-step mode.

## PTP Clocks

Two types of ordinary clocks and boundary clocks are used in this profile:

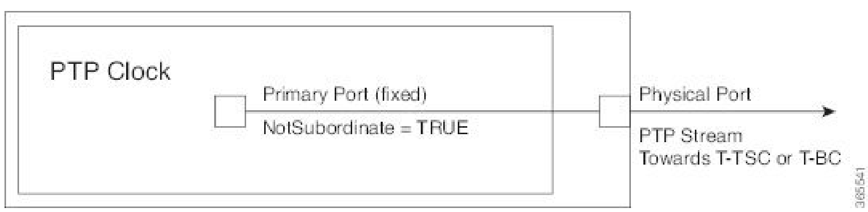
Ordinary Clock (OC)

- OC that can only be a grandmaster clock (T-GM). In this case, one PTP port will be used as a primary port.

The T-GM uses the frequency, 1PPS, and ToD input from an upstream grandmaster clock.

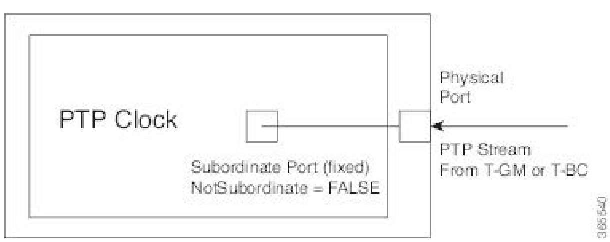
**Note** The T-GM primary port is a fixed primary port.

*Figure 5: Ordinary Clock As T-GM*




- OC that can only be a subordinate clock (T-TSC). In this case, only one PTP port is used for T-TSC, which in turn will have only one PTP primary associated with it.

*Figure 6: Ordinary Clock As Subordinate Clock (T-TSC)*

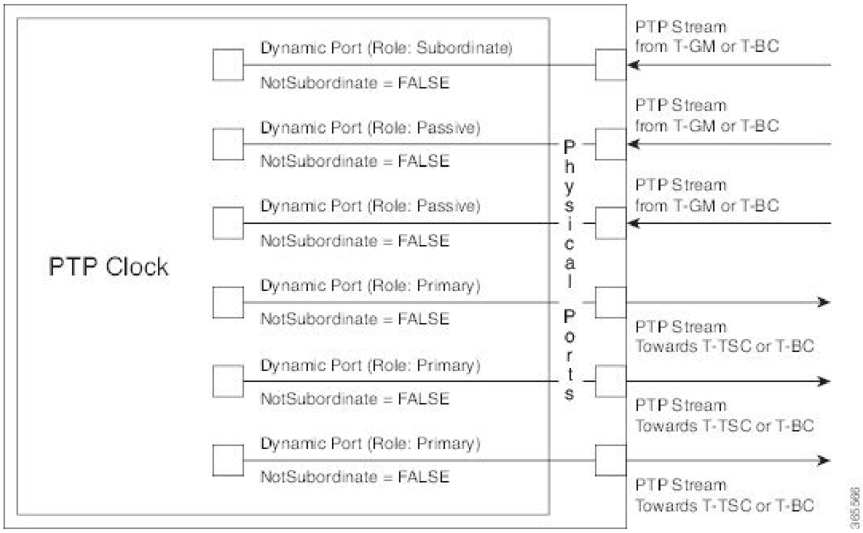



Boundary Clock (T-BC)

1. T-BC that can only be a grandmaster clock (T-GM).
2. T-BC that can become a primary clock and can also be a subordinate clock to another PTP clock.

If the BMCA selects a port on the T-BC to be a subordinate port, all other ports are moved into the primary role or a passive state.

*Figure 7: Boundary Clock*




## PTP Ports

A port can be configured to perform either fixed Server or Client role or can be configured to change its role dynamically. If no role is assigned to a port, it can dynamically assume a server, passive, or client role based on the BMCA.

A server port provides the clock to its downstream peers.

A client port receives clock from an upstream peer.

A dynamic port can work either as a server or a client based on the BMCA decision.

In Cisco's implementation of the G.8275.1:

- OC clocks can support only fixed Server or Client port.
- One PTP port can communicate with only one PTP peer.
- BC can have a maximum of 64 ports. Fixed client ports are not supported on the BC.

## Virtual Port Support on T-BC

G.8275.1 introduces the concept of a virtual port on the T-BC. A virtual port is an external frequency, phase and time input interface on a T-BC, which can participate in the source selection.

## Alternate BMCA

The BMCA implementation in G.8275.1 is different from that in the default PTP profile. The G.8275.1 implementation is called the Alternate BMCA. Each device uses the alternate BMCA to select a clock to synchronize to, and to decide the port states of its local ports.

## Benefits

With upcoming technologies like LTE-TDD, LTE-A CoMP, LTE-MBSFN and Location-based services, eNodeBs (base station devices) are required to be accurately synchronized in phase and time. Having GNSS systems at each node is not only expensive, but also introduces vulnerabilities. The G.8275.1 profile meets the synchronization requirements of these new technologies.

## Prerequisites for Using the G.8275.1 Profile

- PTP over Multicast Ethernet must be used.
- Every node in the network must be PTP aware.
- It is mandatory to have a stable physical layer frequency whilst using PTP to define the phase.
- Multiple active grandmasters are recommended for redundancy.

## Restrictions for Using the G.8275.1 Profile

- PTP Transparent clocks are not permitted in this profile.
- Changing PTP profile under an existing clock configuration is not allowed. Different ports under the same clock cannot have different profiles. You must remove clock configuration before changing the PTP profile. Only removing all the ports under a clock is not sufficient.
- One PTP port is associated with only one physical port in this profile.
- There is no support for BDI and VLAN.
- Signaling and management messages are not used.
- PTP message rates are not configurable.
- Non-hybrid T-TSC and T-BC clock configurations are not supported.

# Configuring the G.8275.1 Profile

**Note** To know more about the commands referenced in this module, see the Cisco IOS Interface and Hardware Component Command Reference or the Cisco IOS Master Command List .

## Configuring Physical Frequency Source

For more information, see the Configuring Synchronous Ethernet ESMC and SSM section in the Clocking and Timing chapter of this book.

# Creating a Server-Only Ordinary Clock

```
ptp clock ordinary domain 24
local-priority 1
priority2 128
clock-port server-port-1
master profile g8275.1
local-priority 1
transport ethernet multicast interface Gig 0/0/1
clock-port server-port-2
master profile g8275.1
```

**Note** It is mandatory that when electrical ToD is used, the **utc-offset** command is configured before configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the server and client clocks.

The following example shows that the utc-offset is configured before configuring the ToD to avoid a delay of 37 seconds between the server and client clocks:

```
ptp clock ordinary domain 0
 utc-offset 37
tod R0 cisco
input 1pps R0
clock-port server-port master
  transport ipv4 unicast interface Loopback0 negotiation
```

## Associated Commands

- ptp clock
- local-priority
- priority2

# Creating an Ordinary Slave

```
ptp clock ordinary domain 24
hybrid
clock-port slave-port
slave profile g8275.1
transport ethernet multicast interface Gig 0/0/0
delay-asymmetry 1000
```

# Creating Dynamic Ports

**Note** Dynamic ports can be created when you do not specify whether a port is master or slave. In such cases, the BMCA dynamically choses the role of the port.

```
ptp clock boundary domain 24 hybrid
time-properties persist 600
```

```
utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
clock-port bc-port-1 profile g8275.1local-priority 1
transport ethernet multicast interface Gig 0/0/0
delay-asymmetry 500
clock-port bc-port-2 profile g8275.1 local-priority 2
transport ethernet multicast interface Gig 0/0/1
delay-asymmetry -800
```

# Configuring Virtual Ports

```
ptp clock boundary domain 24 hybrid
utc-offset 45 leap-second "01-01-2017 00:00:00" offset 1
virtual-port virtual-port-1 profile g8275.1 local-priority 1
input 1pps R0
input tod R0 ntp
```

**Note** It is mandatory that when electrical ToD is used, the **utc-offset** command is configured *before* configuring the **tod R0**, otherwise there will be a time difference of approximately 37 seconds between the primary and subordinate clocks.

## Restrictions for Configuring Virtual Ports

- Virtual port configuration is not allowed under Ordinary Clocks.
- Virtual port configuration is not supported under non-hybrid T-BC cases.

## Associated Commands

- input

# Verifying the Local Priority of the PTP Clock

```
Router# show ptp clock dataset default
CLOCK [Boundary Clock, domain 24]
  Two Step Flag: No
  Clock Identity: 0x2A:0:0:0:58:67:F3:4
  Number Of Ports: 1
  Priority1: 128
  Priority2: 90
  Local Priority: 200
  Domain Number: 24
  Slave Only: No
  Clock Quality:
    Class: 224
    Accuracy: Unknown
    Offset (log variance): 4252
```

# Verifying the Port Parameters

```
Router# show ptp port dataset port
PORT [SERVER]
```

```
  Clock Identity: 0x49:BD:D1:0:0:0:0:0
  Port Number: 0
  Port State: Unknown
  Min Delay Req Interval (log base 2): 42
  Peer Mean Path Delay: 648518346341351424
  Announce interval (log base 2): 0
  Announce Receipt Timeout: 2
  Sync Interval (log base 2): 0
  Delay Mechanism: End to End
  Peer Delay Request Interval (log base 2): 0
  PTP version: 2
  Local Priority: 1
  Not-slave: True
```

# Verifying the Foreign Master Information

```
Router# show platform software ptp foreign-master domain 24
PTPd Foreign Master Information:

Current Master: SLA

Port: SLA
  Clock Identity: 0x74:A2:E6:FF:FE:5D:CE:3F
  Clock Stream Id: 0
  Priority1: 128
  Priority2: 128
  Local Priority: 128
  Clock Quality:
    Class: 6
    Accuracy: Within 100ns
    Offset (Log Variance): 0x4E5D
  Steps Removed: 1
  Not-Slave: FALSE
```

# Verifying Current PTP Time

```
Router# show platform software ptpd tod
PTPd ToD information:

Time: 01/05/70 06:40:59
```

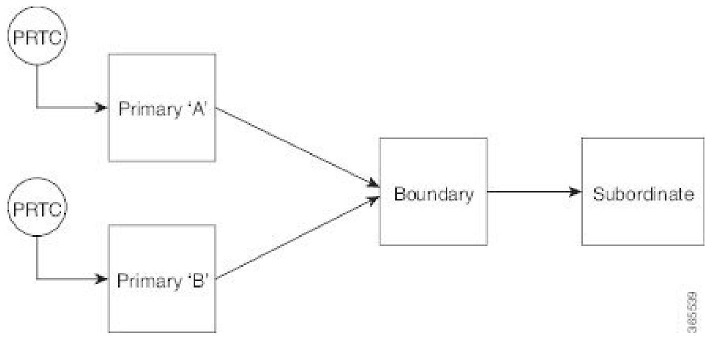
# Verifying the Virtual Port Status

```
Router# show ptp port virtual domain 24
VIRTUAL PORT [vp]
  Status: down
  Clock Identity: 0x74:A2:E6:FF:FE:5D:CE:3F
  Port Number: 1
  Clock Quality:
    Class: 6
    Accuracy: 0x21
    Offset (log variance): 0x4E5D
  Steps Removed: 0
  Priority1: 128
  Priority2: 128
  Local Priority: 128
  Not-slave: False
```

# G.8275.1 Deployment Scenario

The following example illustrates a possible configuration for a G.8275.1 network with two server clocks, a boundary clock and a client. Let's assume that server A is the main server and B is the backup server.

***Figure 8: Topology for a Configuration Example***




The configuration on server clock A is:

```
ptp clock ordinary domain 24
  clock-port server-port profile g8275.1
    transport ethernet multicast interface GigabitEthernet 0/0/0
```

The configuration on server clock B is:

```
ptp clock ordinary domain 25
  clock-port server-port profile g8275.1
```

transport ethernet multicast interface GigabitEthernet 0/1/0

The configuration on the boundary clock is:

```
ptp clock boundary domain 24 hybrid
  local-priority 3
  clock-port client-port-a profile g8275.1 local-priority 1
    transport ethernet multicast interface Gig 0/0/1
  clock-port client-port-b profile g8275.1 local-priority 2
    transport ethernet multicast interface Gig 0/1/1
  clock-port server-port profile g8275.1
    transport Ethernet multicast interface Gig 0/2/1
```

The configuration on the client clock is:

```
ptp clock ordinary domain 24 hybrid
  clock-port client-port slave profile g8275.1
    transport Ethernet multicast interface Gig 0/0/0
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Interface and Hardware Component commands | Cisco IOS Interface and Hardware Component Command Reference |
| Clocking and Timing | Clocking and Timing |

### Standards

| Standard | Title |
|---|---|
| G.8275.1/Y.1369.1 (07/14) | SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS |
| G.8273.2/Y.1368.2 (05/14) | Packet over Transport aspects – Synchronization, quality and availability targets |

### MIBs

| MIB | MIBs Link |
|---|---|
| — | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| — | There are no new RFCs for this feature. |

# Feature Information for G.8275.1

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

**Note** Table 15: Feature Information for G.8275.1 , on page 159 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

*Table 15: Feature Information for G.8275.1*

| Feature Name | Releases | Feature Information |
|---|---|---|
| G.8275.1–Support for 1588 profile | XE 3.18 | This PTP telecom profile introduces phase and time synchronization with full timing support from the network.<br>The following commands were introduced<br>• **local-priority**<br>The following commands were modified:<br>• **clock-port**<br>• **show ptp clock dataset default**<br>• **show ptp port dataset port**<br>The following command is deprecated for the G.8275.1 profile clocks:<br>• **show ptp port running**<br>The alternate command is **show platform software ptp foreign-master [domain-number].**<br>**Note** This command is applicable only for the G.8275.1 profile clocks. |

CHAPTER 11

# Tracing and Trace Management

This chapter contains the following sections:



## Tracing Overview

Tracing is a function that logs internal events. Trace files are automatically created and saved to the tracelogs directory on the harddisk: file system on the chassis, which stores tracing files in bootflash:. Trace files are used to store tracing data.

**Note** The logs in the bootflash are stored in compressed format with .gz file extension. Use the archiving tools such as gunzip, gzip, 7-zip to extract the files.

- If the sytem reloads unexpectedly, some of the files may not be in compressed format.
- Extraction of log files may lead to time hogs or CPU logs. We recommend to perform this by copying the files to the PC.
- Extraction of files *cannot* be performed at the IOS prompt.
- Log files not handled by the bootflash trace are *not* stored in the compressed format (for example, system_shell_R*.log ).

The contents of trace files are useful for the following purposes:

- Troubleshooting—If a chassis is having an issue, the trace file output may provide information that is useful for locating and solving the problem. Trace files can almost always be accessed through diagnostic mode even if other system issues are occurring.
- Debugging—The trace file outputs can help users get a more detailed view of system actions and operations.

# How Tracing Works

The tracing function logs the contents of internal events on the chassis. Trace files with all trace output for a module are periodically created and updated and are stored in the tracelog directory. Trace files can be erased from this directory to recover space on the file system without impacting system performance.

The most recent trace information for a specific module can be viewed using the **show platform software trace message** privileged EXEC and diagnostic mode command. This command can be entered to gather trace log information even during an IOS failure because it is available in diagnostic mode.

Trace files can be copied to other destinations using most file transfer functions (such as FTP, TFTP, and so on) and opened using a plaintext editor.

Tracing cannot be disabled on the chassis. Trace levels, however, which set the message types that generate trace output, are user-configurable and can be set using the **set platform software trace** command. If a user wants to modify the trace level to increase or decrease the amount of trace message output, the user should set a new tracing level using the **set platform software trace** command. Trace levels can be set by process using the **all-modules** keyword within the **set platform software trace** command, or by module within a process. See the **set platform software trace** command reference for more information on this command, and the Tracing Levels, on page 162 of this document for additional information on tracing levels.

# Tracing Levels

Tracing levels determine how much information about a module should be stored in the trace buffer or file.

Table 16: Tracing Levels and Descriptions, on page 162 shows all of the trace levels that are available and provides descriptions of what types of messages are displayed with each tracing level.

***Table 16: Tracing Levels and Descriptions***

| Trace Level | Level Number | Description |
|---|---|---|
| Emergency | 0 | The message is regarding an issue that makes the system unusable. |
| Alert | 1 | The message is regarding an action that must be taken immediately. |
| Critical | 2 | The message is regarding a critical condition. This is the default setting. |
| Error | 3 | The message is regarding a system error. |
| Warning | 4 | The message is regarding a system warning |
| Notice | 5 | The message is regarding a significant issue, but the router is still working normally. |
| Informational | 6 | The message is useful for informational purposes only. |
| Debug | 7 | The message provides debug-level output. |
| Verbose | 8 | All possible tracing messages are sent. |

| Trace Level | Level Number | Description |
|---|---|---|
| Noise | - | All possible trace messages for the module are logged.<br>The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement. |

Trace level settings are leveled, meaning that every setting will contain all messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3(error) ensures that the trace file will contain all output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (warning) will ensure that all trace output for the specific module will be included in that trace file.

The default tracing level for every module on the chassis is notice.

All trace levels are not user-configurable. Specifically, the alert, critical, and notice tracing levels cannot be set by users. If you wish to trace these messages, set the trace level to a higher level that will collect these messages.

When setting trace levels, it is also important to remember that the setting is not done in a configuration mode, so trace level settings are returned to their defaults after every router reload.

**Caution** Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to this level or higher should be done with discretion.

**Caution** Setting a large number of modules to high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

# Viewing a Tracing Level

By default, all modules on the chassis are set to notice. This setting will be maintained unless changed by a user.

To see the tracing level for any module on the chassis, enter the **show platform software trace level** command in privileged EXEC or diagnostic mode.

In the following example, the **show platform software trace level** command is used to view the tracing levels of the Forwarding Manager processes on the active RSP:

```
Router# show platform software trace level forwarding-manager rp active
Module Name                      Trace Level
-----------------------------------------------
acl                              Notice
binos                            Notice
binos/brand                      Notice
bipc                             Notice
bsignal                          Notice
btrace                           Notice
```

```
cce                              Notice
cdllib                           Notice
cef                              Notice
chasfs                           Notice
chasutil                         Notice
erspan                           Notice
ess                              Notice
ether-channel                    Notice
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
fman_rp                          Notice
fpm                              Notice
fw                               Notice
icmp                             Notice
interfaces                       Notice
iosd                             Notice
ipc                              Notice
ipclog                           Notice
iphc                             Notice
ipsec                            Notice
mgmte-acl                        Notice
mlp                              Notice
mqipc                            Notice
nat                              Notice
nbar                             Notice
netflow                          Notice
om                               Notice
peer                             Notice
qos                              Notice
route-map                        Notice
sbc                              Notice
services                         Notice
sw_wdog                          Notice
tdl_acl_config_type              Notice
tdl_acl_db_type                  Notice
tdl_cdlcore_message              Notice
tdl_cef_config_common_type       Notice
tdl_cef_config_type              Notice
tdl_dpidb_config_type            Notice
tdl_fman_rp_comm_type            Notice
tdl_fman_rp_message              Notice
tdl_fw_config_type               Notice
tdl_hapi_tdl_type                Notice
tdl_icmp_type                    Notice
tdl_ip_options_type              Notice
tdl_ipc_ack_type                 Notice
tdl_ipsec_db_type                Notice
tdl_mcp_comm_type                Notice
tdl_mlp_config_type              Notice
tdl_mlp_db_type                  Notice
tdl_om_type                      Notice
tdl_ui_message                   Notice
tdl_ui_type                      Notice
tdl_urpf_config_type             Notice
tdllib                           Notice
trans_avl                        Notice
uihandler                        Notice
uipeer                           Notice
uistatus                         Notice
urpf                             Notice
vista                            Notice
wccp                             Notice
```

# Setting a Tracing Level

To set a tracing level for any module on the chassis, or for all modules within a process, enter the **set platform software trace** privileged EXEC and diagnostic mode command.

In the following example, the trace level for the ACL module in the Forwarding Manager of the ESP processor in slot 0 is set to info.

**set platform software trace forwarding-manager F0 acl info**

See the **set platform software trace** command reference for additional information about the options for this command.

# Viewing the Content of the Trace Buffer

To view the trace messages in the trace buffer or file, enter the **show platform software trace message** privileged EXEC and diagnostic mode command.

In the following example, the trace messages for the Host Manager process in Route Switch Processor slot 0 are viewed using the **show platform software trace message** command:

```
Router# show platform software trace message host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in
 slot 0
```

CHAPTER 12

# OTN Wrapper Overview

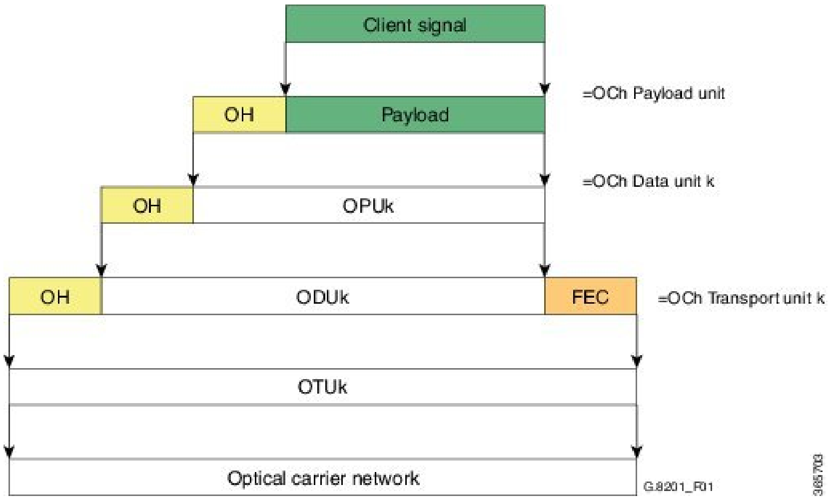
Optical Transport Network (OTN) Wrapper feature provides robust transport services that leverage many of the benefits such as resiliency and performance monitoring, while adding enhanced multi-rate capabilities in support of packet traffic, plus the transparency required by Dense Wavelength Division Multiplexing (DWDM) networks. OTN is the ideal technology to bridge the gap between next generation IP and legacy Time Division Multiplexing (TDM) networks by acting as a converged transport layer for newer packet-based and existing TDM services. OTN is defined in ITU G.709 and allows network operators to converge networks through seamless transport of the numerous types of legacy protocols, while providing the flexibility required to support future client protocols.

OTN Wrapper feature is supported on the following interface modules:

- 8-port 10 Gigabit Ethernet Interface Module (8x10GE) (A900-IMA8Z) (NCS4200-8T-PS) - The encapsulation type is OTU1e and OTU2e.
- 2-port 40 Gigabit Ethernet QSFP Interface Module (2x40GE) (A900-IMA2F) (NCS4200-2Q-P) - The encapsulation type is OTU3.
- 1-port 100 Gigabit Ethernet Interface Module (1X100GE) (NCS4200-1H-PK) (A900-IMA1C) - The encapsulation type is OTU4.

The chassis acts as an aggregator for ethernet, TDM, and SONET traffic to connect to an OTN network and vice versa. The ports on the interface modules are capable of OTN functionality. The OTN controller mode enables the IPoDWDM technology in the interface modules. The OTN Wrapper encapsulates 10G LAN, 40G LAN, and 100G LAN into the corresponding OTU1e or OTU2e, OTU3, and OTU4 containers, respectively. This enables the ports of the interface modules to work in layer 1 optical mode in conformance with standard G.709.

*Figure 9: OTN Signal Structure*




### OTN Frame

The key sections of the OTN frame are the Optical Channel Transport Unit (OTU) overhead section, Optical Channel Data Unit (ODU) overhead section, Optical Channel Payload Unit (OPU) overhead section, OPU payload section, and Forward Error Correction (FEC) overhead section . The network routes these OTN frames across the network in a connection-oriented way. The Overhead carries the information required to identify, control and manage the payload, which maintains the deterministic quality. The Payload is simply the data transported across the network, while the FEC corrects errors when they arrive at the receiver. The number of correctable errors depends on the FEC type.

# Advantages of OTN

The following are the advantages of OTN:

- Provides multi-layer performance monitoring and enhanced maintenance capability for signals traversing multi-operator networks.
- Allows Forward Error Correction (FEC) to improve the system performance.
- Provides enhanced alarm handling capability.
- Insulates the network against uncertain service mix by providing transparent native transport of signals encapsulating all client-management information.
- Performs multiplexing for optimum capacity utilization, thereby improving network efficiency.
- Enables network scalability as well as support for dedicated Ethernet services with service definitions.

# ODU and OTU

Optical Channel Transport Unit (OTU) and Optical Channel Data Unit (ODU) are the two digital layer networks. All client signals are mapped into the optical channel via the ODU and OTU layer networks.

**OTU**

The OTU section is composed of two main sections: the Frame Alignment section and the Section Monitoring (SM) section. The OTU Overhead (OH) provides the error detection correction as well as section-layer connection and monitoring functions on the section span. The OTU OH also includes framing bytes, enabling receivers to identify frame boundaries. For more information, see *G.709 document*.

ODU

The ODU section is an internal element allowing mapping or switching between different rates, which is important in allowing operators the ability to understand how the end user pipe is transferred through to the higher network rates. The ODU OH contains path overhead bytes allowing the ability to monitor the performance, fault type and location, generic communication, and six levels of channel protection based on Tandem Connection Monitoring (TCM). For more information, see *G.709 document*.

# Deriving OTU1e and OTU2e Rates

A standard OTN frame consists of 255 16-column blocks and the payload rate is 9953280 Kbit/s. This is because the overhead and stuffing in the OTN frames happen at a granularity of 16-column blocks. Thus, OPU payload occupies (3824-16)/16=238 blocks. The ODU occupies 239 blocks and the OTU (including FEC) occupies 255 blocks. Hence, the multiplication factor in the G.709 spec is specified using numbers like 237, 238, 255.

Since OPU2e uses 16 columns that are reserved for stuffing and also for payload, the effective OPU2e frequency is:

- OPU2e = 238/237 x 10312500 Kbit/s = 10.356012 Gbit/s
- ODU2e = 239/237 x 10312500 Kbit/s = 10.399525 Gbit/s
- OTU2e = 255/237 x 10312500 Kbit/s = 11.095727 Gbit/s

Since OPU1e uses 16 columns that are reserved for stuffing and also for payload, the effective OPU1e frequency is:

- OPU1e = 238/238 x 10312500 Kbit/s = 10.3125 Gbit/s
- ODU1e = 239/238 x 10312500 Kbit/s = 10.355829 Gbit/s
- OTU1e = 255/238 x 10312500 Kbit/s = 11.049107 Gbit/s

# OTU1e and OTU 2e Support on 8x10GE Interface Module

The OTU1e and OTU2e are mapping mechanisms to map a client 10G Base-R signal to OTN frames transparently as per ITU-T G series Supplement 43 specification. Both these modes are over-clocked OTN modes. These mechanisms provide real bit transparency of 10 GbE LAN signals and are useful for deployment of 10G services.

The OTU1e and OTU2e are inherently intra-domain interfaces (IaDI) and are generally applicable only to a single vendor island within an operator's network to enable the use of unique optical technology. The OTU1e and OTU2e are not standard G.709 bit-rate signals and they do not interwork with the standard mappings of Ethernet using GFP-F. These two over-clocked mechanisms do not interwork with each other. As a result, such signals are only deployed in a point-to-point configuration between equipment that implements the same mapping.

The standard 10 GbE LAN has a data rate of 10.3125 Gbps. In the OTU1e and OTU2e mapping schemes, the full 10.3125 Gbit/s is transported including the 64B/66B coded information, IPG, MAC FCS, preamble, start-of-frame delimiter (SFD) and the ordered sets (to convey fault information). So, the effective OTU2e and OTU1e rates are:

- OTU1e: 11.0491 Gbits/s +/- 100ppm
- OTU2e: 11.0957 Gbits/s +/- 100ppm

The 10GBase-R client signal with fixed stuff bytes is accommodated into an OPU-like signal, then into an ODU-like signal, and further into an OTU-like signal. These signals are denoted as OPU2e, ODU2e and OTU2e, respectively . The OTU1e does not add 16 columns of fixed stuff bytes and hence overall data rate is relatively lesser at 11.0491 Gbps as compared to OTU2e which is 11.0957 Gbps.

The following table shows the standard OTU rates:

*Table 17: Standard OTU Rates*

| G.709 Interface | Line Rate | Corresponding Ethernet Rate | Line Rate |
|---|---|---|---|
| OTU-1e | 11.0491 Gbit/s without stuffing bits | 10 Gig E-LAN | 10.3125 Gbit/s |

| G.709 Interface | Line Rate | Corresponding Ethernet Rate | Line Rate |
|---|---|---|---|
| OTU-2e | 11.0957 Gbit/s without stuffing bits | 10 Gig E-LAN | 10.3125 Gbit/s |
| OTU-3 | 43.018 Gbit/s | STM-256 or OC-768 | 39.813 Gbit/s |

# OTU3 Support in 2x40GE Interface Module

When 40GbE LAN is transported over OTN, there is no drop in line rate when the LAN client is mapped into the OPU3 using the standard CBR40G mapping procedure as specified in G.709 clause 17.2.3. The 40G Ethernet signal (41.25 Gbit/s) uses 64B/66B coding making it slightly larger than the OPU3 payload rate that is 40.15 Gbit/s. Hence, to transport 40G Ethernet service over ODU3, the 64B/66B blocks are transcoded into 1024B/1027B block code to reduce their size. The resulting 40.117 Gbit/s transcoded stream is then mapped in standard OPU3.

# OTU4 Support on 1-port 100 Gigabit Ethernet Interface Module (1X100GE)

A 100G ethernet client signal running at 103.125 Gbit/s rate can be mapped directly into an OPU4 payload area.

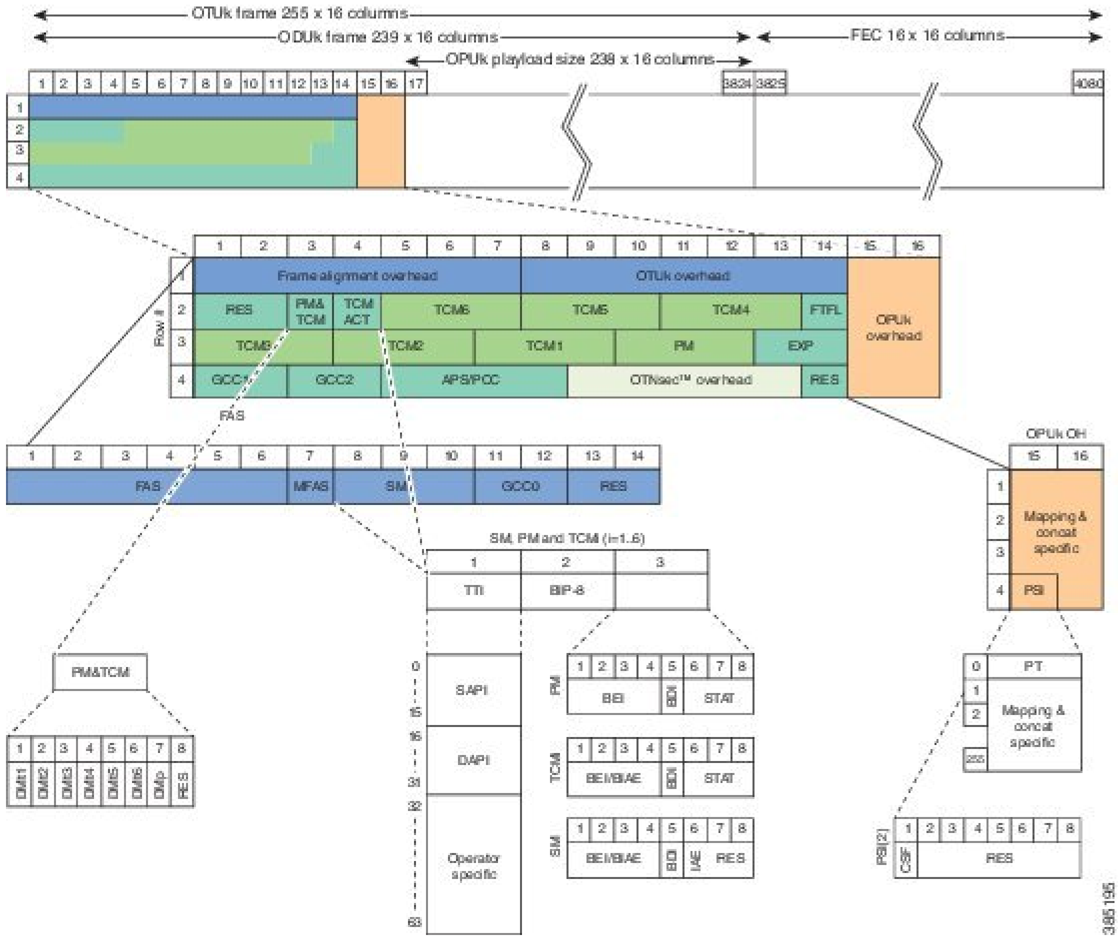
# Supported Transceivers

The OTN wrapper feature works with the standard transceiver types that are supported for the LAN mode of 10G, 40G and 100G on the interface modules. The SFP-10G-LR-X, QSFP-40G-LR4, and CPAK-100G-SR10 are used for 8x10GE, 2x40GE, and 1X100GE interface modules, respectively.

# OTN Specific Functions

The following figure shows the OTN specific functions related to overhead processing, alarm handling, FEC and TTI:

*Figure 10: OTN Specific Functions*




# Standard MIBS

The following are the standard MIBS:

- RFC2665
- RFC1213
- RFC2907
- RFC2233
- RFC3591

# Restrictions for OTN

The following are the restrictions for OTN:

- OTL alarms are not supported.
- FECMISMATCH alarm is not supported.
- Enhanced FEC is not supported.
- Alarm and error counters are visible when the controller is in shutdown state.

# DWDM Provisioning

All DWDM provisioning configurations take place on the controller. To configure a DWDM controller, use the controller dwdm command in global configuration mode.

## Prerequisites for DWDM Provisioning

The g709 configuration commands can be used only when the controller is in the shutdown state. Use the **no shutdown** command after configuring the parameters, to remove the controller from shutdown state and to enable the controller to move to up state.

## Configuring DWDM Provisioning

Use the following commands to configure DWDM provisioning:

```
enable
configure terminal
controller dwdm 0/1/0
```

# Configuring Transport Mode in 8x10GE and 2x40GE Interface Modules

Use the **transport-mode** command in interface configuration mode to configure LAN and OTN transport modes in 8x10GE and 2x40GE interface modules. The **transport-mode** command **otn** option has the bit-transparent sub-option, using which bit transparent mapping into OPU1e or OPU2e can be configured.

Use the following commands to configure LAN and OTN transport modes:

```
enable
configure terminal
controller dwdm 0/0/0
transport-mode otn bit-transparent opu1e
```

**Note** LAN transport mode is the default mode.

To configure the transport administration state on a DWDM port, use the **admin-state** command in DWDM configuration mode. To return the administration state from a DWDM port to the default, use the **no** form of this command.

# Verification of LAN Transport Mode Configuration

Use the **show interfaces** command to verify the configuration of LAN transport mode:

```
Router#sh int te0/1/0
TenGigabitEthernet0/1/0 is up, line protocol is up
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 8/255, rxload 193/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 10000Mbps, link type is force-up, media type is SFP-SR
  output flow-control is unsupported, input flow-control is on
  Transport mode LAN
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 04:02:09, output 04:02:09, output hang never
  Last clearing of "show interface" counters 00:29:47
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 7605807000 bits/sec, 14854906 packets/sec
  5 minute output rate 335510000 bits/sec, 655427 packets/sec
     26571883351 packets input, 1700600465344 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     10766634813 packets output, 689064271464 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

# Verification of OTN Transport Mode Configuration in 8x10GE Interface Modules

Use the **show interfaces** command to verify the configuration of OTN transport mode in 8x10GE interface modules:

```
Router#sh int te0/1/1
TenGigabitEthernet0/1/1 is up, line protocol is up
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 193/255, rxload 7/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 10000Mbps, link type is force-up, media type is SFP-SR
  output flow-control is unsupported, input flow-control is on
  Transport mode OTN (10GBASE-R over OPU1e w/o fixed stuffing, 11.0491Gb/s)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 03:28:14, output 03:28:14, output hang never
  Last clearing of "show interface" counters 00:30:47
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 281326000 bits/sec, 549608 packets/sec
  5 minute output rate 7596663000 bits/sec, 14837094 packets/sec
     10766669034 packets input, 689066159324 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
```

```
     27457291925 packets output, 1757266795328 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

# Verification of OTN Transport Mode Configuration in 2x40GE Interface Modules

Use the **show interfaces** command to verify the configuration of OTN transport mode in 2x40GE interface modules:

```
Router#show int  fo0/4/0
FortyGigabitEthernet0/4/0 is up, line protocol is up
  MTU 1500 bytes, BW 40000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 40000Mbps, link type is force-up, media type is QSFP_40GE_SR
  output flow-control is unsupported, input flow-control is on
  Transport mode OTN OTU3 (43.018Gb/s)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

# Changing from OTN to LAN Mode

Use the following methods to change from OTN mode to LAN mode:

- Use the following commands to make the transport mode as LAN mode:

```
enable
configure terminal
controller dwdm 0/0/0
transport-mode lan
```

- Use the following commands to set the controller default transport mode as LAN mode:

```
enable
configure terminal
```

```
controller dwdm 0/0/0
default transport-mode
```

## Verification of Enabled Ports for Controller Configuration

Use the show controllers command to verify the enables ports for the controller configuration:

```
#show controllers
TenGigabitEthernet0/0/0
TenGigabitEthernet0/0/1
TenGigabitEthernet0/0/2
TenGigabitEthernet0/0/3
TenGigabitEthernet0/0/4
TenGigabitEthernet0/0/5
TenGigabitEthernet0/0/6
TenGigabitEthernet0/0/7
TenGigabitEthernet0/1/0
TenGigabitEthernet0/1/1
FortyGigabitEthernet0/4/0
FortyGigabitEthernet0/4/1
TenGigabitEthernet0/5/0
TenGigabitEthernet0/5/1
TenGigabitEthernet0/5/2
TenGigabitEthernet0/5/3
TenGigabitEthernet0/5/4
TenGigabitEthernet0/5/5
TenGigabitEthernet0/5/6
TenGigabitEthernet0/5/7
#
```

# Configuring Transport Mode in 1X100GE Interface Module

Use the **transport-mode** command in interface configuration mode to configure LAN and OTN transport modes in 1X100GE interface module. The **transport-mode** command *otn* option has the bit-transparent sub-option.

Use the following commands to configure LAN and OTN transport modes:

```
enable
configure terminal
controller dwdm 0/0/0
transport-mode otn otu4 100G
```

**Note** LAN transport mode is the default mode.

To configure the transport administration state on a DWDM port, use the **admin-state** command in DWDM configuration mode. To return the administration state from a DWDM port to the default, use the **no** form of this command.

## Verification of Transport Mode Configuration on 1X100GE Interface Module

Use the following commands to verify the transport mode configuration on 1X100GE interface module:

```
#show interfaces Hu0/8/0
HundredGigE0/8/0 is up, line protocol is up
  Hardware is NCS4200-1H-PK, address is 7426.acf6.8048 (bia 7426.acf6.8048)
  MTU 1500 bytes, BW 100000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100000Mbps, link type is force-up, media type is CPAK-100G-SR10
  output flow-control is off, input flow-control is off
  Transport mode OTN OTU4 (111.80997Gb/s)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out

#

#show controllers dwdm 0/8/0
G709 Information:
Controller dwdm 0/8/0, is up (no shutdown)
Transport mode OTN OTU4
Loopback mode enabled : None
TAS state is : IS
G709 status : Enabled
OTU
        LOS = 0            LOF = 0            LOM = 0
        AIS = 0            BDI = 0            BIP = 0
        TIM = 0            IAE = 0            BEI = 0
ODU
        AIS = 0            BDI = 0            TIM = 0
        OCI = 0            LCK = 0            PTIM = 0
        BIP = 0            BEI = 0
FEC Mode: None
Remote FEC Mode: Unknown
        FECM                            = 0
        EC(current second)              = 0
        EC                              = 0
        UC                              = 0
Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI OTU-TIM ODU-AIS ODU-OCI
ODU-LCK ODU-BDI ODU-PTIM ODU-TIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-6
TCA thresholds: SM = 10e-3  PM = 10e-3
OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
```

```
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000
ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000
```

# OTN Alarms

OTN supports alarms in each layer of encapsulation. All the alarms follow an alarm hierarchy and the highest level of alarm is asserted and presented as a Syslog message or on the CLI.

**OTU Alarms**

The types of alarms enabled for reporting:

- AIS - Alarm indication signal (AIS) alarms
- BDI - Backward defect indication (BDI) alarms
- IAE - Incoming alignment error (IAE) alarms
- LOF - Loss of frame (LOF) alarms
- LOM - Loss of multiple frames (LOM) alarms
- LOS - Loss of signal (LOS) alarms
- TIM - Type identifier mismatch (TIM) alarms
- SM - TCA - SM threshold crossing alert
- SD-BER - SM BER is in excess of the SD BER threshold
- SF-BER - SM BER is in excess of the SF BER threshold

**ODU Alarms**

The types of alarms enabled for reporting:

- AIS - Alarm indication signal (AIS) alarms
- BDI - Backward defect indication (BDI) alarms
- LCK - Upstream connection locked (LCK) error status
- OCI - Open connection indication (OCI) error status
- PM-TCA - Performance monitoring (PM) threshold crossing alert (TCA)
- PTIM - Payload TIM error status

- SD-BER - SM BER is in excess of the SD BER threshold
- SF-BER - SM BER is in excess of the SF BER threshold
- TIM - Type identifier mismatch (TIM) alarms

# Configuring OTN Alarm Reports

By default, all the OTN alarm reports are enabled. To control OTN alarm reports, disable all the alarms and enable the specific alarms.

**Note** You need to shutdown the interface using the **shut** command to configure the alarms.

## Configuring OTU Alarm Reports

Use the following commands to configure OTU alarm reports:

```
enable
configure terminal
controller dwdm 0/4/1
shut
g709 otu report bdi
no shut
end
```

**Note** Fecmismatch is not supported.

**Note** Use **no g709 otu report** command to disable the OTU alarm reports.

### Verification of OTU Alarm Reports Configuration

Use the **show controllers** command to verify OTU alarm reports configuration:

```
#show controllers dwdm 0/4/1
G709 Information:

Controller dwdm 0/4/1, is up (no shutdown)

Transport mode OTN OTU3
Loopback mode enabled : None

TAS state is : IS
G709 status : Enabled
( Alarms and Errors )
OTU
        LOS = 3            LOF = 1            LOM = 0
        AIS = 0            BDI = 0            BIP = 74444
        TIM = 0            IAE = 0            BEI = 37032

ODU
```

```
        AIS = 0            BDI = 0            TIM = 0
        OCI = 0            LCK = 0            PTIM = 0
        BIP = 2            BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown
        FECM                           = 0
        EC(current second)             = 0
        EC                             = 186
        UC                             = 10695




Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-6
TCA thresholds: SM = 10e-3  PM = 10e-3

OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000
```

### Syslog Generation for LOS Alarm

The following example shows the syslog generation for LOS alarm:

```
(config-if)#
*Jan 16 06:32:50.487 IST: %DWDM-4-G709ALARM: dwdm-0/4/1: LOS declared
*Jan 16 06:32:51.048 IST: %LINK-3-UPDOWN: Interface FortyGigabitEthernet0/4/1, changed state
 to down
*Jan 16 06:32:51.489 IST: %DWDM-4-G709ALARM: dwdm-0/4/1: LOF declared
*Jan 16 06:32:51.495 IST: %DWDM-4-G709ALARM: dwdm-0/4/1: LOS cleared
```

## Configuring ODU Alarm Report

Use the following commands to configure ODU alarm reports:

```
enable
configure terminal
controller dwdm 0/4/1
shut
```

```
g709 odu report ais
no shut
end
```

**Note** Use **no g709 odu report** command to disable the ODU alarm reports.

# OTN Threshold

The signal degrade and signal failure thresholds are configured for alerts.

The following types of thresholds are configured for alerts for OTU and ODU layers:

- SD-BER—Section Monitoring (SM) bit error rate (BER) is in excess of the signal degradation (SD) BER threshold.
- SF-BER—SM BER is in excess of the signal failure (SF) BER threshold.
- PM-TCA—Performance monitoring (PM) threshold crossing alert (TCA).
- SM-TCA—SM threshold crossing alert.

## Configuring OTU Threshold

To configure OTU threshold:

```
enable
configure terminal
controller dwdm 0/4/1
shut
g709 otu threshold sm-tca 3
no shut
end
```

**Note** Use **no g709 otu threshold** command to disable OTU threshold.

## Configuring ODU Threshold

To configure ODU threshold:

```
enable
configure terminal
controller dwdm 0/4/1
shut
g709 odu threshold sd-ber 3
no shut
end
```

**Note** Use **no g709 odu threshold** command to disable configuration of ODU threshold.

# Verification of OTU and ODU Threshold Configuration

Use the **show controllers** command to verify OTU and ODU threshold configuration:

```
Router#show controllers dwdm 0/1/2
G709 Information:

Controller dwdm 0/1/2, is up (no shutdown)

Transport mode OTN (10GBASE-R over OPU1e w/o fixed stuffing, 11.0491Gb/s)
Loopback mode enabled : None

TAS state is : UNKNWN
G709 status : Enabled

OTU
        LOS = 0          LOF = 0          LOM = 0
        AIS = 0          BDI = 0          BIP = 0
        TIM = 0          IAE = 0          BEI = 0

ODU
        AIS = 0          BDI = 0          TIM = 0
        OCI = 0          LCK = 0          PTIM = 0
        BIP = 0          BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown
        FECM                           = 0
        EC(current second)             = 0
        EC                             = 0
        UC                             = 0




Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI OTU-TIM ODU-AIS ODU-OCI
ODU-LCK ODU-BDI ODU-PTIM ODU-TIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-6
TCA thresholds: SM = 10e-3  PM = 10e-3

OTU TTI Sent     String SAPI ASCII      : AABBCCDD
OTU TTI Sent     String DAPI ASCII      : AABBCCDD
OTU TTI Sent     String OPERATOR ASCII  : AABBCCDD
OTU TTI Expected String SAPI ASCII      : AABBCCDD
OTU TTI Expected String DAPI ASCII      : AABBCCDD
OTU TTI Expected String OPERATOR HEX    : AABBCCDD
OTU TTI Received String HEX  : 0052414D4553480000000000000000000052414D455348000
                               0000000000000041414242434344440000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : AABBCCDD
ODU TTI Sent     String DAPI ASCII      : AABBCCDD
ODU TTI Sent     String OPERATOR HEX    : 11223344
ODU TTI Expected String SAPI ASCII      : AABBCCDD
ODU TTI Expected String DAPI ASCII      : AABBCCDD
ODU TTI Expected String OPERATOR HEX    : 11223344
ODU TTI Received String HEX  : 0052414D4553480000000000000000000052414D455348000
                               0000000000000011223344000000000000000000000000000
```

```
                              0000000000000000000000000000000

Router#
```

# Configuring OTU Alerts

To configure OTU alerts:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
g709 otu threshold sd-ber
no shutdown
end
```

# Configuring ODU Alerts

To configure ODU alerts:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
g709 otu threshold pm-tca
no shutdown
end
```

# Configuring ODU Alerts

To configure ODU alerts:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 otu
g709 otu threshold
g709 otu threshold pm-tca
no shutdown
end
```

## Verifying Alerts Configuration

Use the show controllers command to verify the alerts configuration:

```
#show controllers dwdm 0/4/1
G709 Information:

Controller dwdm 0/4/1, is down (shutdown)
```

```
Transport mode OTN OTU3
Loopback mode enabled : Line

TAS state is : IS
G709 status : Enabled

OTU
        LOS = 5           LOF = 1           LOM = 0
        AIS = 0           BDI = 0           BIP = 149549
        TIM = 0           IAE = 0           BEI = 74685

ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 2           BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown
        FECM                           = 0
        EC(current second)             = 0
        EC                             = 856
        UC                             = 23165



Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-5
TCA thresholds: SM = 10e-3  PM = 10e-4

OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000
```

# Loopback

Loopback provides a means for remotely testing the throughput of an Ethernet port on the router. You can verify the maximum rate of frame transmission with no frame loss. Two types of loopback is supported:

- Internal Loopback - All packets are looped back internally within the router before reaching an external cable. It tests the internal Rx to Tx path and stops the traffic to egress out from the Physical port.
- Line Loopback - Incoming network packets are looped back through the external cable.

# Configuring Loopback

To configure loopback:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
loopback line
no shutdown
end
```

## Verifying Loopback Configuration

Use the **show controllers** command to verify the loopback configuration:

```
#show controllers dwdm 0/4/1
G709 Information:

Controller dwdm 0/4/1, is up (no shutdown)

Transport mode OTN OTU3
Loopback mode enabled : Line

TAS state is : IS
G709 status : Enabled

OTU
        LOS = 5           LOF = 1           LOM = 0
        AIS = 0           BDI = 0           BIP = 149549
        TIM = 0           IAE = 0           BEI = 74685

ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 2           BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown
        FECM                            = 0
        EC(current second)              = 0
        EC                              = 856
        UC                              = 23165


Detected Alarms: NONE
```

```
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-4
TCA thresholds: SM = 10e-3  PM = 10e-3

OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

#
```

# Forward Error Connection

Forward error correction (FEC) is a method of obtaining error control in data transmission in which the source (transmitter) sends redundant data and the destination (receiver) recognizes only the portion of the data that contains no apparent errors. FEC groups source packets into blocks and applies protection to generate a desired number of repair packets. These repair packets may be sent on demand or independently of any receiver feedback.

Standard FEC is supported on 8x10GE and 2x40GE interface modules.

The packets that can be corrected by FEC are known as Error Corrected Packets. The packets that cannot be corrected by FEC due to enhanced bit errors are known as Uncorrected Packets.

## Benefits of FEC

The following are the benefits of FEC:

- FEC reduces the number of transmission errors, extends the operating range, and reduces the power requirements for communications systems.
- FEC increases the effective systems throughput.
- FEC supports correction of bit errors occurring due to impairments in the transmission medium.

# Configuring FEC

To configure FEC:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 fec standard
no shutdown
end
```

## Verifying FEC Configuration

Use the **show controllers** command to verify FEC configuration:

```
G709 Information:

Controller dwdm 0/4/1, is up (no shutdown)

Transport mode OTN OTU3
Loopback mode enabled : Line

TAS state is : IS
G709 status : Enabled

OTU
        LOS = 5           LOF = 1           LOM = 0
        AIS = 0           BDI = 0           BIP = 149549
        TIM = 0           IAE = 0           BEI = 74685

ODU
        AIS = 0           BDI = 0           TIM = 0
        OCI = 0           LCK = 0           PTIM = 0
        BIP = 2           BEI = 0

FEC Mode: FEC

Remote FEC Mode: Unknown <— This is a limitation by which we do not show the remote FEC
mode
        FECM                          = 0
        EC(current second)            = 0
        EC                            = 856       < — This is the counter for Error
corrected bits .
        UC                            = 23165     <- this is the counter for Uncorrected
 alarms .




Detected Alarms: NONE
Asserted Alarms: NONE
Detected Alerts: NONE
Asserted Alerts: NONE
Alarm reporting enabled for: LOS LOF LOM OTU-AIS OTU-IAE OTU-BDI ODU-AIS ODU-OCI ODU-LCK
ODU-BDI ODU-PTIM ODU-BIP
Alert reporting enabled for: OTU-SD-BER OTU-SF-BER OTU-SM-TCA ODU-SD-BER ODU-SF-BER ODU-PM-TCA
BER thresholds: ODU-SF = 10e-3  ODU-SD = 10e-6  OTU-SF = 10e-3  OTU-SD = 10e-5
TCA thresholds: SM = 10e-3  PM = 10e-4

OTU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
OTU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
```

```
OTU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
OTU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
OTU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
                               000000000000000000000000000000

ODU TTI Sent     String SAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String DAPI ASCII      : Tx TTI Not Configured
ODU TTI Sent     String OPERATOR ASCII  : Tx TTI Not Configured
ODU TTI Expected String SAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String DAPI ASCII      : Exp TTI Not Configured
ODU TTI Expected String OPERATOR ASCII  : Exp TTI Not Configured
ODU TTI Received String HEX  : 0000000000000000000000000000000000000000000000000
                               0000000000000000000000000000000000000000000000000
```

# Trail Trace Identifier

The Trail Trace Identifier (TTI) is a 64-Byte signal that occupies one byte of the frame and is aligned with the OTUk multiframe. It is transmitted four times per multiframe. TTI is defined as a 64-byte string with the following structure:

- TTI [0] contains the Source Access Point Identifier (SAPI) [0] character, which is fixed to all-0s.
- TTI [1] to TTI [15] contain the 15-character source access point identifier (SAPI[1] to SAPI[15]).
- TTI [16] contains the Destination Access Point Identifier (DAPI) [0] character, which is fixed to all-0s.
- TTI [17] to TTI [31] contain the 15-character destination access point identifier (DAPI [1] to DAPI [15]).
- TTI [32] to TTI [63] are operator specific.

**TTI Mismatch**

TTI mismatch occurs when you have enabled path trace and the "received string" is different from the "expected string". This alarm condition stops traffic.

When TTI mismatch occurs, the interface is brought to down state. This is only supported for SAPI and DAPI and is not supported for **User Operator Data** field.

## Configuring TTI

To configure TTI:

```
enable
configure terminal
controller dwdm 0/1/1
shutdown
g709 tti-processing enable
no shutdown
end
```

Trace Identifier Mismatch (TIM) is reported in the Detected Alarms where there is a mismatch in the expected and received string. Action on detection of TIM can be configured in ODU and OTU layers as follows:

```
enable
configure terminal
controller dwdm 0/1/1
shutdown
g709 tti-processing enable otu
```

```
no shutdown
end
```

### Configuring TTI for SAPI DAPI Operator Specific Fields

To configure TTI SAPI, DAPI, and operator specific fields for OTU and ODU layers:

```
enable
configure terminal
controller dwdm 0/1/1
g709 fec standard
g709 otu overhead tti sent ascii sapi AABBCCDD
end
```

### Verification of TTI SAPI DAPI Operator Specific Fields Configuration

Use the show controller command to verify TTI SAPI, DAPI, Operator Specific fields configuration:

```
Router#show controllers dwdm 0/1/1
G709 Information:
Controller dwdm 0/1/1, is up (no shutdown)

Transport mode OTN (10GBASE-R over OPU1e w/o fixed stuffing, 11.0491Gb/s)

<<truncated other output >>

OTU TTI Sent String SAPI ASCII : AABBCCDD
OTU TTI Sent String DAPI ASCII : AABBCCDD
OTU TTI Sent String OPERATOR ASCII : AABBCCDD
OTU TTI Expected String SAPI ASCII : AABBCCDD
OTU TTI Expected String DAPI ASCII : AABBCCDD
OTU TTI Expected String OPERATOR HEX : AABBCCDD
OTU TTI Received String HEX : 0052414D455348000000000000000000000052414D455348000
0000000000000004141424243434444000000000000000000
000000000000000000000000000000

ODU TTI Sent String SAPI ASCII : AABBCCDD
ODU TTI Sent String DAPI ASCII : AABBCCDD
ODU TTI Sent String OPERATOR HEX : 11223344
ODU TTI Expected String SAPI ASCII : AABBCCDD
```

# SNMP Support

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language that is used for monitoring and managing devices in a network.

SNMP sets are not supported for the following tables:

- coiIfControllerTable
- coiOtnNearEndThresholdsTable
- coiOtnFarEndThresholdsTable
- coiFECThresholdsTable

Refer to CISCO-OTN-IF-MIB and *SNMP Configuration Guide* for SNMP support.

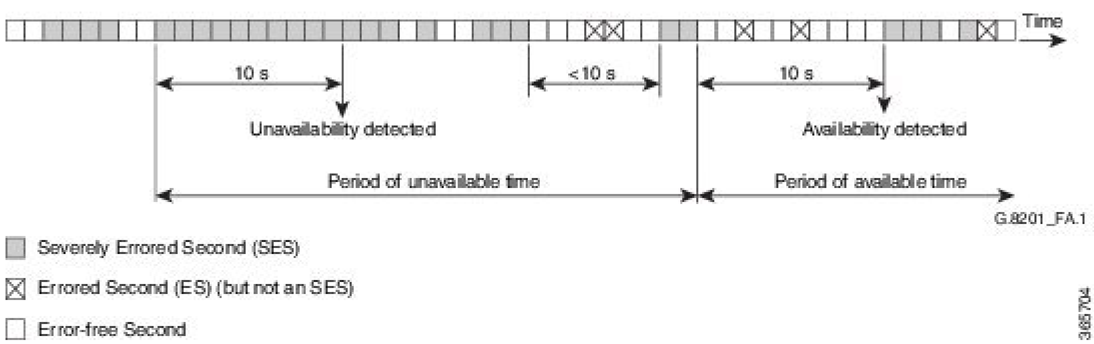
# Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for, and report performance data for early detection of problems. Thresholds are used to set error levels for each PM parameter. During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated. The TCAs provide early detection of performance degradation. PM statistics are accumulated on a 15-minute basis, synchronized to the start of each quarter-hour. Historical counts are maintained for 33 15-minutes intervals and 2 daily intervals. PM parameters are collected for OTN and FEC.

Calculation and accumulation of the performance-monitoring data is in 15-minute and 24-hour intervals.

PM parameters require the errored ratio to be less than the standard reference that is dependent on the encapsulation. If any loss or error event does not happen within a second, it is called an error free second. If some error in transmission or alarm happens in a second, the second is called Errored Second. The error is termed as Errored Second or Severely Errored Second or Unavailable Second depending upon the nature of error. The error calculation depends on the Errored Blocks. Errored second is a second where one BIP error or BEI error occurs. Severely Errored Second occurs when the errored frames crosses a threshold or there is an alarm is generated. Unavaliable Second occurs when there are 10 consecutive severely errored seconds.

*Figure 11: Performance Monitoring*




PM occurs in near end and far end for both encapsulations for ODUk and OTUk. ODU is referred as Path Monitoring (PM) and OTU is referred to as Section Monitoring (SM).

The following table shows the details of each type of PM parameter for OTN:

*Table 18: PM Parameters for OTN*

| Parameter | Definition |
|---|---|
| BBE-PM | Path Monitoring Background Block Errors (BBE-PM) indicates the number of background block errors recorded in the optical transport network (OTN) path during the PM time interval. |
| BBE-SM | Section Monitoring Background Block Errors (BBE-SM) indicates the number of background block errors recorded in the OTN section during the PM time interval. |

| Parameter | Definition |
|---|---|
| BBER-PM | Path Monitoring Background Block Errors Ratio (BBER-PM) indicates the background block errors ratio recorded in the OTN path during the PM time interval. |
| BBER-SM | Section Monitoring Background Block Errors Ratio (BBER-SM) indicates the background block errors ratio recorded in the OTN section during the PM time interval. |
| ES-PM | Path Monitoring Errored Seconds (ES-PM) indicates the errored seconds recorded in the OTN path during the PM time interval. |
| ESR-PM | Path Monitoring Errored Seconds Ratio (ESR-PM) indicates the errored seconds ratio recorded in the OTN path during the PM time interval. |
| ESR-SM | Section Monitoring Errored Seconds Ratio (ESR-SM) indicates the errored seconds ratio recorded in the OTN section during the PM time interval. |
| ES-SM | Section Monitoring Errored Seconds (ES-SM) indicates the errored seconds recorded in the OTN section during the PM time interval. |
| FC-PM | Path Monitoring Failure Counts (FC-PM) indicates the failure counts recorded in the OTN path during the PM time interval. |
| FC-SM | Section Monitoring Failure Counts (FC-SM) indicates the failure counts recorded in the OTN section during the PM time interval. |
| SES-PM | Path Monitoring Severely Errored Seconds (SES-PM) indicates the severely errored seconds recorded in the OTN path during the PM time interval. |
| SES-SM | Section Monitoring Severely Errored Seconds (SES-SM) indicates the severely errored seconds recorded in the OTN section during the PM time interval. |
| SESR-PM | Path Monitoring Severely Errored Seconds Ratio (SESR-PM) indicates the severely errored seconds ratio recorded in the OTN path during the PM time interval. |

| Parameter | Definition |
|---|---|
| SESR-SM | Section Monitoring Severely Errored Seconds Ratio (SESR-SM) indicates the severely errored seconds ratio recorded in the OTN section during the PM time interval. |
| UAS-PM | Path Monitoring Unavailable Seconds (UAS-PM) indicates the unavailable seconds recorded in the OTN path during the PM time interval. |
| UAS-SM | Section Monitoring Unavailable Seconds (UAS-SM) indicates the unavailable seconds recorded in the OTN section during the PM time interval. |

The following table shows the details of each type of PM parameter for FEC:

***Table 19: PM Parameters for FEC***

| Parameter | Definition |
|---|---|
| EC | Bit Errors Corrected (BIEC) indicated the number of bit errors corrected in the DWDM trunk line during the PM time interval. |
| UC-WORDS | Uncorrectable Words (UC-WORDS) is the number of uncorrectable words detected in the DWDM trunk line during the PM time interval. |

# OTUk Section Monitoring

Section Monitoring (SM) overhead for OTUk is terminated as follows:

- TTI
- BIP
- BEI
- BDI
- IAE
- BIAE

BIP and BEI counters are block error counters (block size equal to OTUk frame size). The counters can be read periodically by a PM thread to derive one second performance counts. They are sufficiently wide for software to identify a wrap-around with up to 1.5 sec between successive readings.

The following OTUk level defects are detected:

- dAIS
- dTIM
- dBDI

- dIAE
- dBIAE

Status of the defects is available through CPU readable registers, and a change of status of dLOF, dLOM, and dAIS will generate an interruption.

# ODUk Path Monitoring

Path Monitoring (PM) overhead for higher order ODUk and lower order ODUk is processed as follows:

- TTI
- BIP
- BEI
- BDI
- STAT including ODU LCK/OCI/AIS

The following ODUk defects are detected:

- dTIM
- dLCK and dAIS (from STAT field)
- dBDI

LOS, OTU LOF, OOF and ODU-AIS alarms bring down the interface in system.

# Configuring PM Parameters for FEC

To set TCA report status on FEC layer in 15-minute interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 15-min fec report ec-bits enable
pm 15-min fec report uc-words enable
end
```

To set TCA report status on FEC layer in 24-hour interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 24-hr fec report ec-bits enable
pm 24-hr fec report uc-words enable
end
```

To set threshold on FEC layer in 15-minute interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 15-min fec threshold ec-bits
pm 15-min fec threshold uc-words
end
```

To set threshold on FEC layer in 24-hour interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 24-hr fec threshold ec-bits
pm 24-hr fec threshold uc-words
end
```

# Configuring PM Parameters for OTN

To set OTN report status in 15-minute interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 15-min otn report es-pm-ne enable
end
```

To set OTN report status in 24-hour interval:

```
enable
configure terminal
controller dwdm slot/bay/port
pm 24-hr otn report es-pm-ne enable
end
```

To set OTN threshold in 15-minute interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 15-min otn threshold es-pm-ne
end
```

To set OTN threshold in 24-hour interval:

```
enable
configure terminal
controller dwdm 0/1/0
pm 24-hr otn threshold es-pm-ne
end
```

# Verifying PM Parameters Configuration

Use the **show controllers** command to verify PM parameters configuration for FEC in 15-minute interval:

```
Router#show controllers dwdm 0/1/0 pm interval 15-min fec 0
g709 FEC in the current interval [9 :15:00 - 09:16:40 Thu Jun 9 2016]

FEC current bucket type : INVALID
    EC-BITS   :            0    Threshold :          200   TCA(enable)  : YES
    UC-WORDS  :            0    Threshold :           23  TCA(enable)  : YES


Router#show controllers dwdm 0/1/0 pm interval 15-min fec 1
g709 FEC in interval 1 [9 :00:00 - 9 :15:00 Thu Jun 9 2016]

FEC current bucket type : VALID
    EC-BITS   :            0      UC-WORDS  :            0
```

Use the **show controllers** command to verify PM parameters configuration for FEC in 24-hour interval:

```
Router#show controllers dwdm 0/1/0 pm interval 24 fec 0
g709 FEC in the current interval [00:00:00 - 09:17:01 Thu Jun 9 2016]

FEC current bucket type : INVALID
    EC-BITS   :            0    Threshold :            0   TCA(enable)  : NO
    UC-WORDS  :            0    Threshold :            0  TCA(enable)  : NO


Router#show controllers dwdm 0/1/0 pm interval 24 fec 1
g709 FEC in interval 1 [00:00:00 - 24:00:00 Wed Jun 8 2016]

FEC current bucket type : VALID
    EC-BITS   :          717      UC-WORDS  :      1188574
```

Use the **show controllers** command to verify PM parameters configuration for OTN in 15-minute interval:

```
Router#show controllers dwdm 0/1/0 pm interval 15-min otn 0
g709 OTN in the current interval [9 :15:00 - 09:15:51 Thu Jun 9 2016]

OTN current bucket type: INVALID

OTN Near-End Valid : YES
    ES-SM-NE    :        0     Threshold :        0   TCA(enable)  : NO
    ESR-SM-NE   :  0.00000     Threshold :  0.00010   TCA(enable)  : YES
    SES-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    SESR-SM-NE  :  0.00000     Threshold :  0.02300   TCA(enable)  : NO
    UAS-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBE-SM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBER-SM-NE  :  0.00000     Threshold :  0.02300   TCA(enable)  : NO
    FC-SM-NE    :        0     Threshold :        0   TCA(enable)  : NO
    ES-PM-NE    :        0     Threshold :      200   TCA(enable)  : YES
    ESR-PM-NE   :  0.00000     Threshold :  1.00000   TCA(enable)  : NO
    SES-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    SESR-PM-NE  :  0.00000     Threshold :  0.02300   TCA(enable)  : NO
    UAS-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBE-PM-NE   :        0     Threshold :        0   TCA(enable)  : NO
    BBER-PM-NE  :  0.00000     Threshold :  0.02300   TCA(enable)  : NO
    FC-PM-NE    :        0     Threshold :        0   TCA(enable)  : NO


OTN Far-End Valid : YES
    ES-SM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ESR-SM-FE   :  0.00000       Threshold :  1.00000   TCA(enable)  : NO
    SES-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    SESR-SM-FE  :  0.00000       Threshold :  0.02300   TCA(enable)  : NO
    UAS-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBE-SM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBER-SM-FE  :  0.00000       Threshold :  0.02300   TCA(enable)  : NO
    FC-SM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ES-PM-FE    :        0       Threshold :        0   TCA(enable)  : NO
    ESR-PM-FE   :  0.00000       Threshold :  1.00000   TCA(enable)  : NO
    SES-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    SESR-PM-FE  :  0.00000       Threshold :  0.02300   TCA(enable)  : NO
    UAS-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBE-PM-FE   :        0       Threshold :        0   TCA(enable)  : NO
    BBER-PM-FE  :  0.00000       Threshold :  0.02300   TCA(enable)  : NO
    FC-PM-FE    :        0       Threshold :        0   TCA(enable)  : NO


Router#show controllers dwdm 0/1/0 pm interval 15-min otn 1
g709 OTN in interval 1 [9 :00:00 - 9 :15:00 Thu Jun 9 2016]

OTN current bucket type: VALID
```

```
OTN Near-End Valid : YES        OTN Far-End Valid : YES
    ES-SM-NE    :         0        ES-SM-FE    :         0
    ESR-SM-NE   :  0.00000         ESR-SM-FE   :  0.00000
    SES-SM-NE   :         0        SES-SM-FE   :         0
    SESR-SM-NE  :  0.00000         SESR-SM-FE  :  0.00000
    UAS-SM-NE   :         0        UAS-SM-FE   :         0
    BBE-SM-NE   :         0        BBE-SM-FE   :         0
    BBER-SM-NE  :  0.00000         BBER-SM-FE  :  0.00000
    FC-SM-NE    :         0        FC-SM-FE    :         0
    ES-PM-NE    :         0        ES-PM-FE    :         0
    ESR-PM-NE   :  0.00000         ESR-PM-FE   :  0.00000
    SES-PM-NE   :         0        SES-PM-FE   :         0
    SESR-PM-NE  :  0.00000         SESR-PM-FE  :  0.00000
    UAS-PM-NE   :         0        UAS-PM-FE   :         0
    BBE-PM-NE   :         0        BBE-PM-FE   :         0
    BBER-PM-NE  :  0.00000         BBER-PM-FE  :  0.00000
    FC-PM-NE    :         0        FC-PM-FE    :         0
```

Use the **show controllers** command to verify PM parameters configuration for OTN in 24-hour interval:

```
Router#show controllers dwdm 0/1/0 pm interval 24-hour otn 0
g709 OTN in the current interval [00:00:00 - 09:16:10 Thu Jun 9 2016]

OTN current bucket type: INVALID

OTN Near-End Valid : YES
    ES-SM-NE    :         0     Threshold :         0   TCA(enable)   : NO
    ESR-SM-NE   :  0.00000      Threshold :  0.00000    TCA(enable)   : NO
    SES-SM-NE   :         0     Threshold :         0   TCA(enable)   : NO
    SESR-SM-NE  :  0.00000      Threshold :  0.00000    TCA(enable)   : NO
    UAS-SM-NE   :         0     Threshold :         0   TCA(enable)   : NO
    BBE-SM-NE   :         0     Threshold :         0   TCA(enable)   : NO
    BBER-SM-NE  :  0.00000      Threshold :  0.00000    TCA(enable)   : NO
    FC-SM-NE    :         0     Threshold :         0   TCA(enable)   : NO
    ES-PM-NE    :         0     Threshold :         0   TCA(enable)   : NO
    ESR-PM-NE   :  0.00000      Threshold :  0.00000    TCA(enable)   : NO
    SES-PM-NE   :         0     Threshold :         0   TCA(enable)   : NO
    SESR-PM-NE  :  0.00000      Threshold :  0.00000    TCA(enable)   : NO
    UAS-PM-NE   :         0     Threshold :         0   TCA(enable)   : NO
    BBE-PM-NE   :         0     Threshold :         0   TCA(enable)   : NO
    BBER-PM-NE  :  0.00000      Threshold :  0.00000    TCA(enable)   : NO
    FC-PM-NE    :         0     Threshold :         0   TCA(enable)   : NO


OTN Far-End Valid : YES
    ES-SM-FE    :         0       Threshold :         0   TCA(enable)   : NO
    ESR-SM-FE   :  0.00000        Threshold :  0.00000    TCA(enable)   : NO
    SES-SM-FE   :         0       Threshold :         0   TCA(enable)   : NO
    SESR-SM-FE  :  0.00000        Threshold :  0.00000    TCA(enable)   : NO
    UAS-SM-FE   :         0       Threshold :         0   TCA(enable)   : NO
    BBE-SM-FE   :         0       Threshold :         0   TCA(enable)   : NO
    BBER-SM-FE  :  0.00000        Threshold :  0.00000    TCA(enable)   : NO
    FC-SM-FE    :         0       Threshold :         0   TCA(enable)   : NO
    ES-PM-FE    :         0       Threshold :         0   TCA(enable)   : NO
    ESR-PM-FE   :  0.00000        Threshold :  0.00000    TCA(enable)   : NO
    SES-PM-FE   :         0       Threshold :         0   TCA(enable)   : NO
    SESR-PM-FE  :  0.00000        Threshold :  0.00000    TCA(enable)   : NO
    UAS-PM-FE   :         0       Threshold :         0   TCA(enable)   : NO
    BBE-PM-FE   :         0       Threshold :         0   TCA(enable)   : NO
    BBER-PM-FE  :  0.00000        Threshold :  0.00000    TCA(enable)   : NO
    FC-PM-FE    :         0       Threshold :         0   TCA(enable)   : NO
```

```
Router#show controllers dwdm 0/1/0 pm interval 24-hour otn 1
g709 OTN in interval 1 [00:00:00 - 24:00:00 Wed Jun 8 2016]

OTN current bucket type: INVALID

OTN Near-End Valid : YES        OTN Far-End Valid : NO
    ES-SM-NE    :        7         ES-SM-FE    :        0
    ESR-SM-NE   :  0.00000         ESR-SM-FE   :  0.00000
    SES-SM-NE   :        7         SES-SM-FE   :        0
    SESR-SM-NE  :  0.00000         SESR-SM-FE  :  0.00000
    UAS-SM-NE   :       41         UAS-SM-FE   :        0
    BBE-SM-NE   :        0         BBE-SM-FE   :        0
    BBER-SM-NE  :  0.00000         BBER-SM-FE  :  0.00000
    FC-SM-NE    :        3         FC-SM-FE    :        0
    ES-PM-NE    :        2         ES-PM-FE    :        1
    ESR-PM-NE   :  0.00000         ESR-PM-FE   :  0.00000
    SES-PM-NE   :        0         SES-PM-FE   :        0
    SESR-PM-NE  :  0.00000         SESR-PM-FE  :  0.00000
    UAS-PM-NE   :        0         UAS-PM-FE   :        0
    BBE-PM-NE   :        3         BBE-PM-FE   :        1
    BBER-PM-NE  :  0.00000         BBER-PM-FE  :  0.00000
    FC-PM-NE    :        0         FC-PM-FE    :        0
```

If TCA is enabled for OTN or FEC alarm, a syslog message is displayed for the 15-minute or 24-hour interval as follows:

```
*Jun  9 09:18:02.274: %PMDWDM-4-TCA: dwdm-0/1/0: G709 ESR-SM NE value (540) threshold (10)
 15-min
```

# Troubleshooting Scenarios

The following table shows the troubleshooting solutions for the feature.

| Problem | Solution |
|---|---|
| Link is not coming up | Perform shut and no shut actions of the interface.<br>Check for TTI Mismatch.<br>Verify the major alarms.<br>Verify the FEC mode.<br>Verify that Cisco supported transreceiver list is only used on both sides . |
| Incrementing BIP Error | Verify FEC Mismatch. |
| FEC contains UC and EC errors and link is not coming up | Verify the FEC Mismatch. |

# Associated Commands

The following commands are used to configure OTN Wrapper:

| Commands | Links |
|---|---|
| **controller dwdm** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-c2.html#wp1680149833 |
| **g709 disable** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp7175256270 |
| **g709 fec** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3986227580 |
| **g709 odu report** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3893551740 |
| **g709 odu threshold** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3365653610 |
| **g709 otu report** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3306168000 |
| **g709 otu threshold** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp2500217585 |
| **g709 overhead** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp6997702360 |
| **g709 tti processing** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-f1.html#wp3679037909 |
| **pm fec threshold** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp8624772760 |
| **pm otn report** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp2518071708 |
| **pm otn threshold** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-o1.html#wp1512678519 |
| **show controller dwdm** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s2.html#wp7346292950 |

| Commands | Links |
| --- | --- |
| **show interfaces** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s4.html#wp2987586133 |
| **transport-mode** | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-t1.html#wp3012872075 |

CHAPTER 13

# Using Zero Touch Provisioning

The router provides you the option of having the router auto configure. Field technicians need only mount the router, connect to the power and attach cables in easily-accessible ports, and initiate zero touch provisioning. This feature helps operators to reduce total cost of ownership (TCO) by simplifying the network deployment.

**Note** ZTP is supported only on the RSP3 module on the NCS 4206-16 Series routers.

ZTP is supported on the NCS 4201-4202 routers.

**Note** Routers running ZTP must be able to connect to a DHCP server and a TFTP server, download the configuration template, and begin operation.

**Note** ZTP must be initiated only from the R0 that has the active RSP module in a dual RSP scenario.



# Prerequisites for Using ZTP

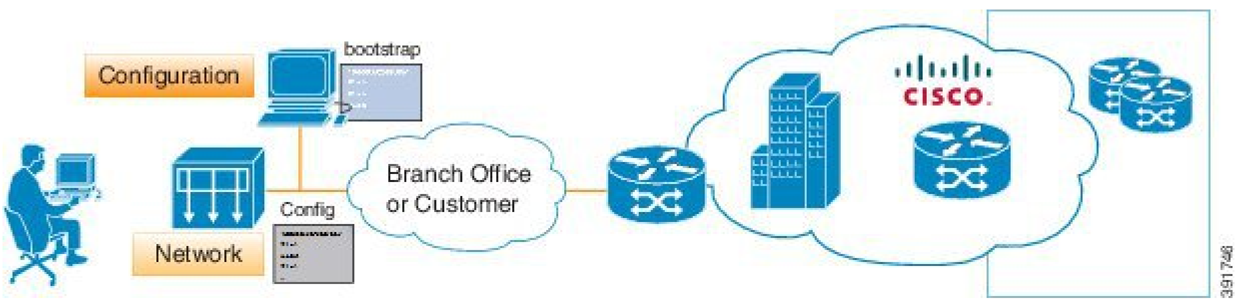
- The connection between the DHCP server or relay and TFTP server and router must be established.
- The TFTP server must have the required network configuration file stored and should be accessible to the router.

# Restrictions for Using ZTP

- ZTP is not supported on the LAN Management port—Gig0 on the router. ZTP is supported only on the Ethernet interfaces such as 1—Gige, 10—Gige ports, and so on.
- ZTP is also not initialized when the router is already reloading or if the router is in ROMMON prompt.
- After the ZTP process completes, you must save the configs using write memory and then reload the router.
- ZTP is not initialized if bootflash has files named as 'router-confg'.
- Disabling gratuitous ARP is not supported.

# Information About Using ZTP

***Figure 12: Sample ZTP Topology***




ZTP is triggered under any of the following conditions:

- A router without a start up configuration is powered on
- The **write erase** and **reload** commands are executed
- The **test platform hardware pp active ztp init** command is executed

The router does *not* have a ZTP or Reset button.

```
Router# write erase
System configuration has been modified. Save? [yes/no]: no
Router# reload
```

**Note** If you type **yes** at the prompt, the system configuration is saved in the nvRAM and the ZTP process terminates.

After the ZTP process initializes, the following sequence is initiated:

1. The router waits for any of the following packet types through data ports to detect the management VLAN:
   - Broadcast (Gratuitous ARP)
   - ISIS hello packets

- OSPF hello packets
- IPv6 router advertisement packets
- VRRP

**Note** The operations center can initiate any of the above packets over the network to establish a connection to the DHCP server.

2. When the first packet on any VLAN is detected, the router initiates a DHCP session to a DHCP server over that VLAN.
3. After a DHCP session is established, the router uses the DHCP option 150 and initiates to download a configuration file from the TFTP server. The configuration file in the TFTP server should have anyone of the following naming format:
   a. PID-*chassis-mac-address*

      The PID specifies NCS and *chassis-mac-address* specifies the unique chassis MAC address printed on the chassis. For example, if the chassis mac-address is 00-01-02-03-04-06, then the config file would be NCS-00-01-02-03-04-05.
   b. network-confg
   c. router-confg
   d. ciscortr.cfg
   e. cisconet.cfg

When the ZTP process initiates, the router creates an Ethernet flow point (EFP) and associates a bridge domain interface (BDI) on the detected management VLAN.

The router creates the following configuration to establish a connection with the DHCP server and the TFTP server. The BDI created for this purpose has description **ZTP_BDI** configured under the BDI interface.

**Note** Once the configuration file is downloaded successfully, you must save the configuration file (write memory) and reload the router.

**Caution** You may choose to remove the **ZTP_BDI** configuration before reloading the router.

# Example ZTP Configuration

Let us assume that GigabitEthernet0/0/1 is connected to the DHCP server and is used to connect to the TFTP server. VLAN ID 1000 is used as the management VLAN.

```
Router# show running-config int gi0/0/1
```

```
Building configuration...
Current configuration : 216 bytes
!
interface GigabitEthernet0/0/1
 no ip address
 media-type auto-select
 no negotiation auto
 service instance 12 ethernet
  encapsulation dot1q 1000
  rewrite ingress tag pop 1 symmetric
  bridge-domain 12
 !
end
!
interface BDI12
description ZTP_BDI
 ip address dhcp
end
```

# Downloading the Initial Configuration

After the VLAN discovery process is complete, the configuration download process begins. The following sequence of events is initiated.

1. The router sends DHCP discover requests on each Ethernet interface. The serial number of the router is used as a client identifier.
2. The DHCP server allocates and sends an IP address, TFTP address (if configured with option 150) and default router address to the router.
3. If the TFTP option (150) is present, the router requests a bootstrap configuration that can be stored in any of the following files: , network-confg, router-confg, ciscortr.cfg, or cisconet.cfg.

**Note** Ensure to use hyphenated hexadecimal notation of MAC address (DOM-78-72-5D-00-A5-80) to name the files.

Effective Cisco IOS XE Amsterdam 17.3.2a, the router tries to learn the reachability to multiple DHCP servers during ZTP. Hence multiple DHCP discovery messages are sent out during this phase. The router goes through all the DHCP offer messages received and selects an appropriate DHCP server based on the priority decided based on below rules:

1. The DHCP server reachable via untagged interface have higher priority than the one via tagged. In case of tagged, the one reachable via an interface learned using VRRP packets has higher priority.
2. If multiple DHCP servers are reachable via similar interfaces mentioned in previous rule, the one reachable via higher physical port number has higher priority.

## DHCP Server

The following is a sample configuration to set up a Cisco router as a DHCP server:

```
ip dhcp excluded-address 30.30.1.6
```

```
ip dhcp excluded-address 30.30.1.20 30.30.1.255
!
ip dhcp pool mwrdhcp
network 30.30.1.0 255.255.255.0
option 150 ip 30.30.1.6
default-router 30.30.1.6
```

This configuration creates a DHCP pool of 30.30.1.*x* addresses with 30.30.1.0 as the subnet start. The IP address of the DHCP server is 30.30.1.6. Option 150 specifies the TFTP server address. In this case, the DHCP and TFTP server are the same.

The DHCP pool can allocate from 30.30.1.1 to 30.30.1.19 with the exception of 30.30.1.6, which is the DHCP server itself.

## TFTP Server

The TFTP server stores the bootstrap configuration file.

The following is a sample configuration (network– confg file):

```
hostname test-router
!
{ncs router-specifc configuration content}
!
end
```

# ZTP LED Behavior

| Process | PWR LED | STAT LED |
|---|---|---|
| Press ZTP button | Green | Blinking Amber |
| Loading image | Blinking Green/Red | OFF |
| Image loaded | Green | Green |
| ZTP process running | Green | Blinking Amber |
| ZTP process success and config-file download completes | Green | Green |
| ZTP process failure or terminated | Green | Red |

# Verifying the ZTP Configuration

To verify if the ZTP configuration is successful, use the following command:

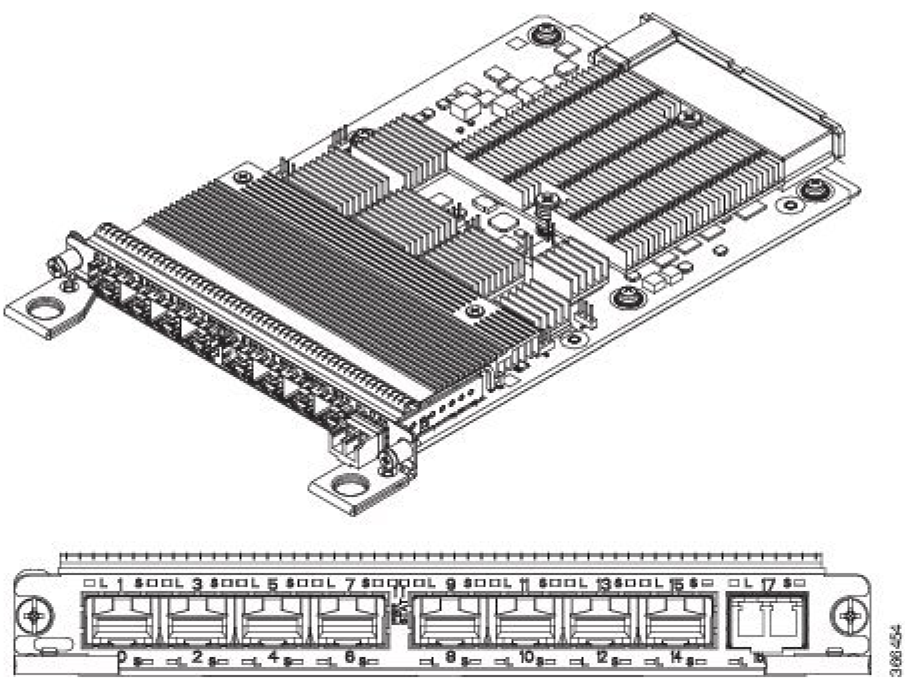
- **show running-config**

CHAPTER 14

# Configuring 8/16-port 1 Gigabit Ethernet (SFP / SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module

The 8/16-port 1 Gigabit Ethernet (SFP / SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module has 8 ports of 1 Gigabit Ethernet and 1 port of 10 Gigabit . The 8/16-port 1 Gigabit Ethernet (SFP / SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module operates on multiple port densities and operating modes. Each physical port can be extended to have 2 ports of 1 Gigabit Ethernet with the use of Compact Small Form-Factor Pluggable (CSFP) module to address high-density port requirements in FTTx deployments.

*Figure 13: 8/16-port 1 Gigabit Ethernet (SFP / SFP) + 1-port 10 Gigabit Ethernet (SFP+) / 2-port 1 Gigabit Ethernet (CSFP) Interface Module*



Each port on CSFP acts as Transmitter or Receiver and connects to GLC-BX-U SFPs using a single strand fiber. GLC-BX-U SFPs support digital optical monitoring (DOM) functions according to the industry-standard SFF-8472 multisource agreement (MSA). This feature gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

**Note** CSFP must be connected only to GLC-BX-U.

This interface module has 8 physical ports of 1 Gigabit Ethernet and 1 physical port of 10 Gigabit Ethernet, but with the support of CSFP, it can support a maximum of 18 ports of 1 Gigabit Ethernet. Thus, the interface module offers enhanced bandwidth.

The following table shows the type of SFPs for 1G and 10G Modules.

*Table 20: Type of SFPs for 1G and 10G Modules*

| Module | Optics |
|---|---|
| 1G Module | SFP |
| | CSFP |
| 10G Module | SFP+ |
| | SFP |
| | CSFP |



# Operating Modes

The interface module supports the following two operating modes:

- Full Subscription
- Over Subscription

**Note** The interface module supports 8 ports of 1 Gigabit Ethernet + 1 port of 10 Gigabit Ethernet mode by default (except the slots 0, 1, 6, and 9 with XFI Pass through mode).

# Full Subscription Mode

Full subscription operating mode supports the bandwidth equal to the number of ports configured.

For example, if you configure 8-port 1GE + 1-port 10GE in full subscription operating mode, then the supported bandwidth is 8 Gigabit Ethernet and 10 Gigabit Ethernet.

The supported operating modes of Full Subscription for ASR 903 NCS 4206 Routers are:

- 16-port 1GE + 1-port 10GE
- 8-port 1GE + 1-port 10 GE
- 18-port 1GE

The supported operating modes of Full Subscription for ASR 907 NCS 4216 Routers are:

- 8-port 1GE + 1-port 10GE
- 8-port 1GE + 1-port 1GE
- 8-port 1GE
- 1-port 10GE

# Over Subscription Mode

Over Subscription operating mode is applicable to 1 Gigabit Ethernet ports only. 16-port 1GE and 16-port 1GE + 1-port 10GE operating modes support 8 Gigabit Ethernet and 18 Gigabit Ethernet bandwidth, respectively. 18-port 1GE supports 9 Gigabit Ethernet bandwidth. But, if the total bandwidth exceeds the supported bandwidth, it results in low priority traffic drop.

For example, if you configure 16-port 1GE + 1-port 10GE over subscription operating mode, then 8GE bandwidth is suported for 16 ports of 1 Giagabit Ethernet and 10GE bandwidth is supported for 10 Giagabit Ethernet ports.

The following are the supported operating modes of Over Subscription for NCS 4216 Routers:

- 16-port 1GE
- 16-port 1GE + 1-port 10GE
- 18-port 1GE

**Note** In 18-port 1GE mode, 10 Gigabit Ethernet physical port slot becomes 2 ports of 1 Gigabit Ethernet with insertion of CSFP.

**Note** By default, the interface module loads in 8-port 1GE + 1-port 10 GE modes (except the slots 0, 1, 6, and 9 with XFI-Pass Through mode. For more information, refer Optics Matrix.

**Note** Over subscription mode is *not* supported on NCS 4206 Routers.

Traffic is classified as follows:

- High Priorty Traffic — Has high priority queue

  This is classified as follows:

  - DMAC=01-80-C2-xx-xx-xx
  - Etype=0x8100, 9100, 9200, 88A8 Cos values=5, 6, 7
  - Etype=0806 (ARP), 88F7 (PTP)
  - Etype=0x800, TOS 5, 6, 7
  - Etype=0x8847, MPLS EXP 5, 6, 7

- Low Priority Traffic — Traffic that does not satisfy the above conditions has low priority queue

## Egress Packet Classifiers

During oversubscription, the egress direction classifies the packet based on the following:

- The first 8 ports use the priority-based flow-control (PFC) to ensure that there are no drop in packets.
- The remaining ports do strict priority between High Priority and Low Priority counters.

**Note** The threshold value is 6 by default (packet with CoS/EXP/DSCP value greater than or equal to 6 is classified as High Priority.

# SADT Mode

For more information on SADT mode, see IP SLA—Service Performance Testing.

# Bandwidth Mode

Each interface module subslot can be assigned a bandwidth. You can reserve the slots with specific bandwidth so that the inetrface module that consumes more than the configured bandwidth is not used.

**Note** The bandwidth mode is *not* supported on ASR 903 Routers and is *only* supported on ASR 907 Routers.

The following table shows the interface module slots for the bandwidth mode.

| IM Subslot | Bandwidth Mode | SADT Operating Mode |
|---|---|---|
| 0 | 8 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 10 Gbps | XFI-Pass Through Mode |
| 1 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | XFI-Pass Through Mode |
| 2 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 18 Gbps | Port Expansion Mode |
| | 20 Gbps | XFI-Pass Through Mode |
| 3 | Not Available | NA |
| 4 | Not Available | NA |
| 5 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 18 Gbps | Port Expansion Mode |
| | 20 Gbps | XFI-Pass Through Mode |
| 6 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 18 Gbps | Port Expansion Mode |
| 7 | 80 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 100 Gbps | Port Expansion Mode or XFI-Pass Through Mode |

| IM Subslot | Bandwidth Mode | SADT Operating Mode |
|---|---|---|
| 8 | 80 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 100 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| 9 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 18 Gbps | Port Expansion Mode |
| 10 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 18 Gbps | Port Expansion Mode |
| | 20 Gbps | XFI-Pass Through Mode |
| 11 | Not Available | NA |
| 12 | Not Available | NA |
| 13 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 18 Gbps | Port Expansion Mode |
| | 20 Gbps | XFI-Pass Through Mode |
| 14 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 18 Gbps | Port Expansion Mode |
| | 20 Gbps | XFI-Pass Through Mode |
| 15 | 8 Gbps | Port Expansion Mode |
| | 10 Gbps | Port Expansion Mode or XFI-Pass Through Mode |
| | 18 Gbps | Port Expansion Mode |
| | 20 Gbps | XFI-Pass Through Mode |

# Slot Support on Operating Modes

The following table shows the slots supported on different operating modes on ASR 907 NCS 4216 Routers.

| IM Subslot | SADT Operating Mode | IM Operating Modes |
|---|---|---|
| 0, 1 | Port Expansion Mode | Unsupported |
| | XFI-Pass Through Mode | 8-port 1GE + 1-port 1GE |
| | | 8-port 1GE |
| | | 16-port 1GE Over Subscribed |
| | | 18-port 1GE Over Subscribed |
| 2, 5, 10, 13, 14, 15 | XFI-Pass Through Mode | 8-port 1GE + 1-port 10GE |
| | | 16-port 1GE + 1-port 10GE Over Subscribed |
| | Any | 8-port 1GE + 1-port 1GE |
| | | 8-port 1GE |
| | | 16-port 1GE Over Subscribed |
| | | 18-port 1GE Over Subscribed |
| | | 1-port 10GE |
| 3, 4, 7, 8, 11, 12 | Any | 8-port 1GE + 1-port 10GE |
| | | 8-port 1GE + 1-port 1GE |
| | | 8-port 1GE |
| | | 1-port 10GE |
| | | 16-port 1GE + 1-port 10GE Over Subscribed |
| | | 16-port 1GE Over Subscribed |
| | | 18-port 1GE Over Subscribed |
| 6, 9 | Any | 8-port 1GE + 1-port 1GE |
| | | 8-port 1GE |
| | | 1-port 10GE |
| | | 16-port 1GE Over Subscribed |
| | | 18-port 1GE Over Subscribed |

The following table shows the slots supported for different operating modes for ASR 903 routers.

| IM Subslot | IM Operating Modes |
| --- | --- |
| 0, 3, 4, and 5 | 16-port 1GE + 1-port 10GE Fully Subscribed |
| | 8-port 1GE + 1-port 10GE |
| | 18-port 1GE Fully Subscribed |
| 1, 2 | Unsupported |

# IOS Port Numbering

The IOS port numbers are different from other typical interface module because of the flexibility of optics choices and operating modes. The IOS port number is even numbered for SFP optics (for example, Gigabit Ethernet 0/x/0) and the additional port on CSFP insertion introduces the odd number (for example, Gigabit Ethernet 0/x/0 and Gigabit Ethernet 0/x/1) as enumerated in the table below.

***Table 21: IOS Port Number***

| 1G Face Plate Port | SFP Optics | CSFP Optics |
| --- | --- | --- |
| 0 | Gigabit Ethernet 0/x/0 | Gigabit Ethernet 0/x/0 and Gigabit Ethernet 0/x/1 |
| 1 | Gigabit Ethernet 0/x/2 | Gigabit Ethernet 0/x/2 and Gigabit Ethernet 0/x/3 |
| 2 | Gigabit Ethernet 0/x/4 | Gigabit Ethernet 0/x/4 and Gigabit Ethernet 0/x/5 |
| 3 | Gigabit Ethernet 0/x/6 | Gigabit Ethernet 0/x/6 and Gigabit Ethernet 0/x/7 |
| 4 | Gigabit Ethernet 0/x/8 | Gigabit Ethernet 0/x/8 and Gigabit Ethernet 0/x/9 |
| 5 | Gigabit Ethernet 0/x/10 | Gigabit Ethernet 0/x/10 and Gigabit Ethernet 0/x/11 |
| 6 | Gigabit Ethernet 0/x/12 | Gigabit Ethernet 0/x/12 and Gigabit Ethernet 0/x/13 |
| 7 | Gigabit Ethernet 0/x/14 | Gigabit Ethernet 0/x/14 and Gigabit Ethernet 0/x/15 |

Similarly, the IOS port number on the 10G module also has an even number and the additional port on CSFP insertion is odd numbered as listed in the table below.

*Table 22: IOS Port Number*

| 10G Face Plate Port | SFP+ | SFP (1G BW) | CSFP (1G BW) |
|---|---|---|---|
| 8 | Ten Gigabit Ethernet 0/x/16 | Ten Gigabit Ethernet 0/x/16 | Ten Gigabit ethernet 0/x/16 and Gigabit Ethernet 0/x/17 |

# Suported Features on the Interface Module

- Supports PTP implementation. PTP is supported on 1G SFP, 10G SFP+, and CSFP ports.
- Supports SyncE.
- Supports both full subscription and over subscription modes.
- Provides multiple combinations of port density in Full subscription and Over Subscription modes.

# Benefits

- The interface module has enhanced port density.
- 10 GE port can also operate in 1GE mode.

# Restrictions

- In XFI Pass through mode, the interface module goes out of service without any mode configuration on slots 0, 1, 6, and 9. Configure the supported modes on the slots before inserting the interface module.
- This interface module is supported only on Cisco RSP3 module.
- OTN, Wan Phy, and MACsec are *not* supported.
- High Priority Traffic with frame size more than 4500 bytes is *not* supported for oversubscription mode.
- COS, EXP, and DSCP fields in frames with values 5, 6, and 7 respectively, are considered as High Priority Traffic for Oversubscription mode than other control packets.
- 1 G Module ports must have symmetric configuration on both local and peer ends for the ports to come up on the router. For example, if autonegotiation is configured on the local end, it must be configured on the peer end.

# Configuring Interface Module

To configure interface module:

```
enable
hw-module subslot 0/4 default
```

```
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface GigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
configure terminal
platform hw-module configuration
hw-module 0/4  NCS4200-1T16G-PS mode mode
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface GigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
```

# Example: Configuring Full Subscription Modes

The following are the examples to configure different modes of full subscription.

**8-port 1GE + 1-port 10GE Full Subscription Mode Configuration**:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
```

```
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 8x1G+1x10G-FS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

**8-port 1GE + 1-port 1GE Full Subscription Mode Configuration**:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
```

```
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 8x1G+1x1G-FS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
```

**8-port 1GE Full Subscription Mode Configuration**:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 8x1G-FS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
```

```
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

**1-port 10GE Full Subscription Mode Configuration**:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 1x10G-FS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
```

```
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

# Example: Configuring Over Subscription Modes

The following are the examples to configure different modes of over subscription.

**16-port 1GE + 1-port 10GE Over Subscription Mode Configuration**:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 16x1G+1x10G-OS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

**18-port 1GE Over Subscription Mode Configuration**:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 18x1G-OS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

**16-port 1GE Over Subscription Mode Configuration**:

```
Router# enable
Router#hw-module subslot 0/4 default
Proceed with setting all interfaces as default for the module? [confirm]%Setting all
interfaces in 0/4 to default state
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
```

```
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration

Router# configure terminal
Router(config)#platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/4  NCS4200-1T16G-PS mode 16x1G-OS
Interface configs would be defaulted before mode change followed by a soft reset of IM,
will take ~3 min to complete initialization.
----------Do you wish to continue?----------? [yes]: y
Please wait ~3 mins before applying any configs on the IM
Interface GigabitEthernet 0/4/0 set to default configuration
Interface GigabitEthernet 0/4/1 set to default configuration
Interface GigabitEthernet 0/4/2 set to default configuration
Interface GigabitEthernet 0/4/3 set to default configuration
Interface GigabitEthernet 0/4/4 set to default configuration
Interface GigabitEthernet 0/4/5 set to default configuration
Interface GigabitEthernet 0/4/6 set to default configuration
Interface GigabitEthernet 0/4/7 set to default configuration
Interface GigabitEthernet 0/4/8 set to default configuration
Interface GigabitEthernet 0/4/9 set to default configuration
Interface GigabitEthernet 0/4/10 set to default configuration
Interface GigabitEthernet 0/4/11 set to default configuration
Interface GigabitEthernet 0/4/12 set to default configuration
Interface GigabitEthernet 0/4/13 set to default configuration
Interface GigabitEthernet 0/4/14 set to default configuration
Interface GigabitEthernet 0/4/15 set to default configuration
Interface TenGigabitEthernet 0/4/16 set to default configuration
Interface GigabitEthernet 0/4/17 set to default configuration
#
```

# Example: Configuring Egress Classification

**Note** PFC (priority-based flow-control) and egress classification are enabled by default.

The following configuration shows how to modify an egress classification:

```
int gi 0/15/8
flowcontrol egress classify all threshold 7

flowcontrol egress classify ?
            all   classify based on L2-CoS, MPLS-EXP and L3-DSCP
            l2    classify based on L2-CoS
            l3    classify based on L3-DSCP precedence bits
            mpls  classify based on MPLS-EXP

qos-overhead-accounting enable gigabitEthernet 0/15/1
qos-overhead-accounting positive 4
```

# Verifying PFC

Use the show platform hardware pp active bshell command to verify the PFC (priority-based flow-control).

```
show platform hardware pp active bshell "show counters full"
T_127.xl7                   :         1,410,242,436             +2,365
903/sTPOK.xl7               :         1,410,242,436             +2,365
903/sTPKT.xl7               :         1,410,242,436             +2,365
903/sTUCA.xl7               :         1,410,242,436             +2,365
903/sTBYT.xl7               :        95,896,485,648           +160,820
61,375/sR_64.xe134          :               390,320               +786
299/sRPKT.xe134             :               916,242               +786
299/sRXCF.xe134             :               390,320               +786
299/sRXPP.xe134             :               390,320               +786
299/sRPFC_0.xe134           :               362,115               +786
299/sRPFC_1.xe134           :               362,925               +786
299/sRPFC_2.xe134           :               361,555               +786
299/sRPFC_3.xe134           :               362,454               +786
299/sRPFC_4.xe134           :               363,298               +786
299/sRPFC_5.xe134           :               361,532               +786
299/sRPFC_6.xe134           :               362,606               +786
299/sRPFC_7.xe134           :               362,034               +786
299/sRBYT.xe134             :           100,972,834            +50,304
```

# Verifying Configuration

Use the **show platform hw-configuration** command to verify the operating modes configured on the interface module.

```
Router#show platform hw-configuration
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State Op Mode
BW
------ ------------------- ------------------- ------------------ -------- ------------
------------        --
 0/0   -                   -                   Empty              N/A      -

 0/1   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G-OS

 0/2   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       18x1G-OS

 0/3   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G

 0/4   -                   -                   Empty              N/A      -

 0/5   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       18x1G-OS

 0/6   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G-OS

 0/7   -                   -                   Empty              N/A      -

 0/8   -                   -                   Empty              N/A      -

 0/9   -                   -                   Empty              N/A      -

 0/10  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS

 0/11  -                   -                   Empty              N/A      -

 0/12  -                   -                   Empty              N/A      -

 0/13  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS
```

```
 0/14  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS

 0/15  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS


Router#show platform hw-configuration
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State Op Mode
BW
------ ------------------- ------------------- ------------------ -------- ------------
--
 0/0   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/1   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/2   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/3   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G

 0/4   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/5   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/6   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/7   -                   NCS4200-1H-PK       IS-NR              IS       -

 0/8   -                   NCS4200-1H-PK       IS-NR              IS       -

 0/9   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/10  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/11  -                   -                   Empty              N/A      -

 0/12  -                   -                   Empty              N/A      -

 0/13  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/14  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/15  NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS
```

# Verifying High Priority and Low Priority Counters Configuration

Use **show platform software agent iomd** [*IM module*] **fpga dump** [*port number*] to display the packets of High Priority and Low Priority traffice queue in Over Subscription mode.

```
#show platform software agent iomd 0/8 fpga dump 4
OS LP Drop Q Pkt Cnt :0x0
OS HP Drop Q Pkt Cnt :0x0
OS LP Q Pkt Cnt :0x22906bd0
OS HP Q Pkt Cnt :0x55fdd731
```

Use **show platform software agent iomd** [*IM module*] **fpga clear** [*port number*] to clear High Priority and Low Priority counters in Over Subscription mode.

```
#show platform software agent iomd 0/8 fpga clear 4
OS LP Drop Q Pkt Cnt :0x0
OS HP Drop Q Pkt Cnt :0x0
```

```
OS LP Q Pkt Cnt :0x0
OS HP Q Pkt Cnt :0x0
```

# Configuring Bandwidth Mode

To configure bandwidth mode:

```
enable
configure terminal
platform hw-module configuration
bandwidth 0/0 8-gbps
end
```

## Verifying Bandwidth Mode Configuration

Use **show platform hw-configuration** command to verify bandwidth mode configuration.

```
#show platform hw-configuration
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State Op Mode      BW

------ ------------------- ------------------- ------------------ -------- ------------ --
 0/0   -                   -                   Empty              N/A      -
 0/1   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G-OS
 0/2   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       18x1G-OS
 0/3   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G
 0/4   -                   -                   Empty              N/A      -
 0/5   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       18x1G-OS
20-gbps
 0/6   A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G-OS
 0/7   -                   -                   Empty              N/A      -
 0/8   -                   -                   Empty              N/A      -
 0/9   -                   -                   Empty              N/A      -
 0/10  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS
 0/11  -                   -                   Empty              N/A      -
 0/12  -                   -                   Empty              N/A      -
 0/13  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS
 0/14  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS
 0/15  A900-IMA8CS1Z-M     A900-IMA8CS1Z-M     IS-NR              IS       16x1G+1x10G-OS
#
```

```
#show platform hw-configuration
Slot   Cfg IM Type         Actual IM Type      Op State           Ad State Op Mode
BW
------ ------------------- ------------------- ------------------ -------- ------------
--
 0/0   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS
10-gbps
 0/1   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/2   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G

 0/3   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G

 0/4   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/5   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       16x1G+1x10G-OS

 0/6   NCS4200-1T16G-PS    NCS4200-1T16G-PS    IS-NR              IS       18x1G-OS

 0/7   -                   NCS4200-1H-PK       IS-NR              IS       -
```

```
0/8   -                  NCS4200-1H-PK      IS-NR            IS      -
0/9   NCS4200-1T16G-PS   NCS4200-1T16G-PS   IS-NR            IS      18x1G-OS
0/10  NCS4200-1T16G-PS   NCS4200-1T16G-PS   IS-NR            IS      16x1G+1x10G-OS
0/11  -                  -                  Empty            N/A     -
0/12  -                  -                  Empty            N/A     -
0/13  NCS4200-1T16G-PS   NCS4200-1T16G-PS   IS-NR            IS      16x1G+1x10G-OS
0/14  NCS4200-1T16G-PS   NCS4200-1T16G-PS   IS-NR            IS      16x1G+1x10G-OS
0/15  NCS4200-1T16G-PS   NCS4200-1T16G-PS   IS-NR            IS      16x1G+1x10G-OS
```

# Interface Module Rules

**NCS 4206 ASR 903 Routers or Cisco RSP3C-400-S Rules for A900-IMA8CS1Z NCS4200-1T16G-PS**

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 0 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16 x 1GigE (CSFP) + 1 x 10GigE (SFP+) Fully subscribed<br>• 18-port 1GE Fully subscribed | The IM cannot be in slot 0 if IMA1C is in slot 4 |
| 1 | Not Supported | — |
| 2 | Not Supported | — |
| 3 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1 x 10GE (SFP+) Fully subscribed<br>• 18-port 1GE Fully subscribed | — |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 4 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 18-port 1GE Fully subscribed | — |
| 5 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 18-port 1GE Fully subscribed | — |

### NCS 4216 ASR 907 Routers or Cisco RSP3C (Port Expansion Mode) Rules for A900-IMA8CS1Z NCS4200-1T16G-PS

**Note**

- If IMA8S, IMA8T, IMA8S1Z, and IMA8T1Z are in any slot, SADT cannot be configured.
- If the IMA8CS1Z interface module is not present in a slot, mode update through hw sub-slot mode is not allowed. The existing mode configuration applies to the interface module that is reinserted, and you can subsequently update the mode.

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 0 | Not supported | — |
| 1 | Not supported | — |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 2 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10GE Fully subscribed | For Slot 2 in 8-port 1GE Fully Subscribed or 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode, IMA8Z or IMA2F cannot be in slot 4. |
| 3 | All modes are supported | If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15. |
| 4 | All modes are supported | If IMA8Z or IMA2F is present in slot 4, the IM cannot be used in slots 2, 6, 10 and 14. |
| 5 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10G Fully subscribed | If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15. |
| 6 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10G Fully subscribed | If IMA8Z or IMA2F is present in slot 4, the IM cannot be used in slots 2, 6, 10 and 14. |
| 7 | All modes are supported | — |
| 8 | All modes are supported | — |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 9 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10G Fully subscribed | If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15. |
| 10 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10G Fully subscribed | If IMA8Z or IMA2F is present in slot 4, the IM cannot be used in slots 2, 6, 10 and 14. |
| 11 | All modes are supported | If the IM is in slot 11, IMA8S, IMA8T, IMA8S1Z, and IMA8T1Z cannot be used in slots 1, 5, 9, 13 and 15. |
| 12 | All modes are supported | If the IM is in slot 12, IMA8S, IMA8T, IMA8S1Z, and IMA8T1Z cannot be used in slots 0, 2, 6, 10 and 14. |
| 13 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10G Fully subscribed | If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15. |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 14 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10G Fully subscribed | If IMA8Z or IMA2F is present in slot 4, the IM cannot be used in slots 2, 6, 10 and 14. |
| 15 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10G Fully subscribed | If IMA8Z or IMA2F is present in slot 3, the IM cannot be used in slots 5, 9, 13 and 15. |

**NCS 4216 ASR 907 Routers or Cisco RSP3C (XFI-Pass Through Mode) for A900-IMA8CS1Z NCS4200-1T16G-PS**

**Note** IMA8S, IMA8T, IMA8S1Z, and IMA8T1Z cannot be used in any slot.

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 0 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed | • If the IM is in slot 0 in 8-port 1GE Fully subscribed mode or in 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, the IM in Slot 12 can only be in 8-port 1GE (SFP) Fully subscribed mode or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, 1-port 10GE Fully subscribed mode.<br>• If Slot 0 is in 8-port 1G Fully subscribed mode or 16-port/18-port 1GE, or 16-port/18-port 1G Over subscribed or 1-port 10G Fully subscribed mode or 8-port 1G + 1-port 1G Fully subscribed mode.<br>• If Slot 0 is in 8-port 1G Fully subscribed mode or 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, then IMA8Z or IMA2F cannot be in slot 12.<br>• IF IMA8CS1Z-M is in slot 0, then NCS4200 1T8S-10CS (10G_CEM) in slot 12 is not supported.<br>• IF IMA8CS1Z-M is in slot 0 then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported. |
| 1 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed | • If Slot 1 is in 8-port 1G Fully subscribed or 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, the IMA8Z or IMA2F or IMA2Z cannot be in slot 11.<br>• If the IM is in slot 1, then NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported.<br>• If the IM is in slot 1, then NCS4200-1T8S-10CS (5G_CEM) in slot 11 is supported. |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 2 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed<br>• 16-port/18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10G Fully subscribed<br>• 8-port 1GE Fully subscribed | • If Slot 2 is in 8-port 1G + 1-port 10G Fully subscribed mode, or 16-port 1G + 1-port 10G Over subscribed mode, then no IM can be present in slot 12.<br>• If Slot 2 is in 8-port 1G + 1-port 10G Fully subscribed mode, or 16-port 1G + 1-port 10G Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 4.<br>• If the IM in slot 2, then NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported.<br>• If the IM is in slot 2, then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is not supported.<br>• If the IM is in slot 2 then NCS4200-48T1E1-CE in slot 12 is not supported.<br>• If the IM is in slot 2 then NCS4200-48T3E3-CE in slot 12 is not supported. |
| 3 | All modes are supported. | • If IMA8Z or IMA2F is in slot 3, then the IM is not supported on slots 5, 9, 13, and 15.<br>• If Slot 3 has IMA8Z or IMA2F, then no IM can be present in slots 5, 9, 13, and 15. |
| 4 | All modes are supported. | • If IMA8Z or IMA2F is in slot 4, then the IM is not supported in slots 2, 6, 10, and 14.<br>• If Slot 4 has IMA8Z or IMA2F, then no IM can be present in slots 2, 6, 10, and 14. |
| 5 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Over subscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10GE Fully subscribed<br>• 8-port 1GE Fully subscribed | • If the IM is in slot 5 in 8-port 1GE + 1-port 10GE Fully subscribed mode or in 16-port 1GE + 1-port 10GE Oversubscribed mode, the the IM in slot 11 can only be in 8-port 1GE Fully subscribed mode or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, or 1-port 10 GE Fully subscribed mode.<br>• If Slot 5 is in 8-port 1G + 1-port 10G Fully subscribed, or 16-port 1G + 1-port 10G Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 3.<br>• If the IM is in slot 5, then NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported.<br>• If the IM is in slot 5, then NCS4200-1T8S-10CS (5G_CEM) in slot 11 is supported. |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 6 | • 8-port 1GE (SFP) Fully subscribed mode<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10 GE Fully subscribed | • If Slot 6 is in 8-port 1GE fully subscribed, or 16-port 1GE Over subscribed, or 18-port 1GE Over subscribed or 8-port 1GE + 1-port 1GE fully subscribed or 1-port 10GE Fully subscribed mode, then IMA8Z or IMA2F cannot be in slot 4. |
| 7 | All modes are supported | — |
| 8 | All modes are supported | — |
| 9 | • 8-port 1GE (SFP) Fully subscribed<br>• 16-port/18-port 1GE (CSFP) Oversubscribed<br>• 16-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10 GE Fully subscribed | If Slot 9 is in 8-port 1GE fully subscribed, or 16-port 1GE Over subscribed mode, or 18-port 1GE Over subscribed mode or 8-port 1GE + 1-port 1GE fully subscribed or 1-port 10GE Fully subscribed mode, then IMA8Z or IMA2F cannot be in slot 3. |
| 10 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed<br>• 16-port/18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE+1-port 1GE Fully subscribed<br>• 1-port 10 GE Fully subscribed<br>• 8-port 1G Fully subscribed | • If Slot 10 and 14 are in 8-port 1GE + 1-port 10GE Fully subscribed, or 16-port 1GE + 1-port 10GE Over subscribed mode, then IMA8Z IMA2F cannot be in Slot 4.<br>• If IM is in slot 10 then NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported.<br>• If IM is in slot 10, then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported. |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 11 | All modes are supported | |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| | | • IM can be in slot 11, only in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, or 1-port 10 GE Fully subscribed mode if IPSEC is used (FLSASR907-IPSEC).<br>• If the IM is slot 11, and in 8-port 1GE + 1 x 10GigE Fully subscribed mode, or in 16-port 1GE + 1-port 10GE Oversubscribed mode, then the IM in Slots 5 and 15 can only be in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE +1-port 1GE Fully subscribed or 1-port 10GE Fully subscribed mode.<br>• If the IM is in slot 11, and in 8-port 1GE Fully subscribed mode, or in 16-port 1GE Oversubscribed mode, or in 18-port 1GE Oversubscribed mode or in 8-port 1GE + 1-port 1GE Fully subscribed or 1-port 10GE Fully subscribed, then the IM in Slot 15 can only be in 8-port 1GE (SFP) Fully subscribed mode, OR in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 1-port 10GE Fully subscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode.<br>• IF IMA2Z is in slot 11, then the IM is in slot 15 only in 8-port 1GE (SFP) Fully subscribed mode, OR in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode, and no IM can be present in slot 1.<br>• If IMA8Z or IMA2Fis in slot 11, then the IM is in slots 5, 13 and 15 in 8-port 1GE Fully Subscribed, or in 16-port/18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode, and no IM can be present in slot 1.<br>• If NCS4200-1T8S-10CS (10G_CEM) is in slot 11, then the IM in slots 5, 13 and 15 are in only 8-port 1GE Fully Subscribed, or in 16/18-port 1GE Oversubscribed mode, and the IM in slot 1 not supported.<br>• If NCS4200-1T8S-10CS (5G_CEM) is in slot 11, then the IM in slot 15 is in only 8-port 1GE Fully Subscribed, OR in 16/18-port 1GE Oversubscribed mode.<br>• If NCS4200-48T1E1-CE is in slot 11, then the IM is in slot 15 is in only 8-port 1GE Fully Subscribed, or |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| | | in 16/18-port 1GE Oversubscribed mode.<br>• If NCS4200-48T3E3-CE is in slot 11, then the IM is in slot 15 is in only 8-port 1GE Fully Subscribed, or in 16-port/18-port 1GE Oversubscribed mode. |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 12 | All modes are supported | |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| | | • If the IM is in slot 12, and in 8-port 1GE + 1-port 10GE Fully subscribed mode, or in 16-port 1GE + 1-port 10GE Oversubscribed mode, then no IM can be present in Slot 0, and the IM in Slot 2 can only be in 8-port 1GE (SFP) Fully subscribed mode, OR in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode.<br>• If the IM is in slot 12 and in 8-port 1GE Fully subscribed mode or in 16-port 1GE Oversubscribed mode, or in 18-port 1GE Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode, then the IM in Slot 2 can only be in 8-port 1GE (SFP) Fully subscribed mode, OR in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode.<br>• IF IMA2Z is in slot 12, then the IM is in slots 2 and 10 in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode or 1-port 10GE Fully subscribed mode.<br>• If Slot 12 has IMA2Z, then slots 2 and 10 in 8-port 1GE Fully subscribed mode, or 16-port/18-port 1GE Over subscribed mode or 1-port 10GE Fully subscribed mode or 8-port 1G + 1-port 1GE Fully subscribed mode.<br>• If IMA8Z OR IMA2F is in slot 12, then the IM in slots 2, 10 and 14 in 8-port 1GE Fully Subscribed, or in 16-port/18-port 1GE Oversubscribed mode and 1-port 10GE Fully subscribed mode or 8-port 1GE + 1-port 1GE Fully subscribed mode, and no IM can be present from Slot 1 to Slot 0.<br>• If NCS4200-1T8S-10CS (10G_CEM) is in slot 12, then the IM in slots 2, 10 and 14 are in only 8-port 1GE Fully Subscribed, OR in 16-port/18-port 1GE Oversubscribed mode, and the IM in slot 0 not supported.<br>• If NCS4200-1T8S-10CS (5G_CEM) is in slot 12, then the IM in slot 2 is in only 8-port 1GE Fully Subscribed, OR in 16-port/18-port 1GE Oversubscribed mode.<br>• If NCS4200-48T1E1-CE is in slot 12, then the IM in slot 2 is in only 8-port 1GE Fully Subscribed, OR in 16-port/18-port 1GE Oversubscribed mode. |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| | | • If NCS4200-48T3E3-CE is in slot 12, then the IM in slot 2 is in only 8-port 1GE Fully Subscribed, or in 16-port/18-port 1GE Oversubscribed mode. |
| 13 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed<br>• 16-port/18-port 1GE (CSFP Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10 GE Fully subscribed<br>• 8-port 1G Fully subscribed | • If IPSEC is used (FLSASR907-IPSEC) then the IM can be in slot 13, only in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode. NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported; but NCS4200-1T8S-10CS (5G_CEM) in slot 11 is supported.<br>• If the IM in slot 13 is configured in 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed mode, or in 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed mode, or Fully Subscribed mode, then IPSEC cannot be configured.<br>If Slot 13 is in 8-port 1GE + 1-port 10GE Fully subscribed mode, or 16-port 1GE + 1-port 10GE Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 3.<br>• If the IM is in slot 13, then NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported.<br>• If the IM is in slot 13, then NCS4200-1T8S-10CS (5G_CEM) in slot 11 is supported. |
| 14 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed<br>• 16-port/18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10 GE Fully subscribed<br>• 8-port 1GE Fully subscribed | • IF 10G Y.1564/SADT is used, then the IM can be in slot 14 only in 8-port 1GE (SFP) Fully subscribed mode, or in 16-port/18-port 1GE (CSFP) Oversubscribed mode, or 8-port 1GE + 1-port 1GE Fully subscribed mode, or 1-port 10GE Fully subscribed mode. NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported, but NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported.<br>• If Slot 14 is in 8-port 1GE + 1-port 10GE Fully subscribed mode or 16-port 1GE + 1-port 10GE Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 4.<br>• If the IM is in slot 14, then NCS4200-1T8S-10CS (10G_CEM) in slot 12 is not supported.<br>• If the IM is in slot 14, then NCS4200-1T8S-10CS (5G_CEM) in slot 12 is supported. |

| Slot Number | Supported IM Operating Modes | Restrictions |
|---|---|---|
| 15 | • 8-port 1GE (SFP) + 1-port 10GE (SFP+) Fully subscribed<br>• 16-port 1GE (CSFP) + 1-port 10GE (SFP+) Oversubscribed<br>• 16-port/18-port 1GE (CSFP) Oversubscribed<br>• 8-port 1GE + 1-port 1GE Fully subscribed<br>• 1-port 10 GE Fully subscribed<br>• 8-port 1GE Fully subscribed | • IF IMA8CS1Z-M is in slot 15 in 8-port 1GE + 1-port 10GE Fully subscribed mode, or in 16-port 1GE + 1-port 10GE Oversubscribed mode, then the IM cannot be present in slot 11.<br>• If Slot 15 is in 8-port 1GE + 1-port 10GE Fully subscribed mode, or 16-port 1GE + 1-port 10GE Over subscribed mode, then no IM is supported on slot 11.<br>• If Slot 15 is in 8-port 1GE + 1-port 10GE Fully subscribed, Or 16-port 1GE + 1-port 10GE Over subscribed mode, then IMA8Z or IMA2F cannot be in slot 3.<br>• If the IM is in slot 15, then NCS4200-1T8S-10CS (10G_CEM) in slot 11 is not supported.<br>• If the IM is in slot 15, then NCS4200-1T8S-10CS (5G_CEM) in slot 11 is not supported.<br>• If the IM is in slot 15, then NCS4200-48T1E1-CE in slot 11 is not supported.<br>• If the IM is in slot 15, then NCS4200-48T3E3-CE in slot 11 is not supported. |

# Associated Commands

The following table shows the Associated Commands for interface module configuration:

| Commands | Links |
|---|---|
| **show platform software agent iomd** [*im module*] **dump fpga** [*port number*] | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s5.html#wp6318513600 |
| **show platform software agent iomd** [*im module*] **clear fpga** [*port number*] | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/command/ir-cr-book/ir-s5.html#wp6318513600 |

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |

| Related Topic | Document Title |
| --- | --- |
| Compact-SFP | Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet |

### Standards and RFCs

| Standard/RFC | Title |
| --- | --- |
| — | *There are no standards and RFCs for this feature.* |

### MIBs

| MIB | MIBs Link |
| --- | --- |
| — | *There are no MIBs for this feature.*<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
| --- | --- |
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |